# Bitdefender®
# TOTAL SECURITY

User's Guide

Copyright© 2013 Bitdefender

# Bitdefender Total Security
*User's Guide*

Publication date 08/12/2013

Copyright© 2013 Bitdefender

## Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

**Warning and Disclaimer.** This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

**Trademarks.** Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.

Bitdefender

# Table of Contents

Installation ..... 1
1. Preparing for installation ..... 2
2. System requirements ..... 3
2.1. Minimum system requirements ..... 3
2.2. Recommended system requirements ..... 3
2.3. Software requirements ..... 3
3. Installing your Bitdefender product ..... 5
Getting started ..... 10
4. The basics ..... 11
4.1. Opening the Bitdefender window ..... 11
4.2. Fixing issues ..... 12
4.2.1. Fix All Issues wizard ..... 12
4.2.2. Configuring status alerts ..... 13
4.3. Events ..... 13
4.4. Autopilot ..... 15
4.5. Game Mode and Laptop Mode ..... 15
4.5.1. Game Mode ..... 16
4.5.2. Laptop Mode ..... 18
4.6. Password-protecting Bitdefender settings ..... 18
4.7. Anonymous usage reports ..... 19
5. Bitdefender interface ..... 20
5.1. System tray icon ..... 20
5.2. Main window ..... 21
5.2.1. Upper toolbar ..... 22
5.2.2. Panels area ..... 23
5.3. Settings Overview window ..... 27
5.4. Security Widget ..... 28
5.4.1. Scanning files and folders ..... 29
5.4.2. Hide / show Security Widget ..... 29
5.5. Security Report ..... 30
5.5.1. Checking the Security Report ..... 31
5.5.2. Turning on or off the Security Status notification ..... 32
6. Registering Bitdefender ..... 33
6.1. Entering your license key ..... 33
6.2. Buying or renewing license keys ..... 33
7. MyBitdefender account ..... 35
7.1. Linking your computer to MyBitdefender ..... 35
8. Keeping Bitdefender up-to-date ..... 38
8.1. Checking if Bitdefender is up-to-date ..... 38
8.2. Performing an update ..... 39

8.3. Turning on or off automatic update . . . . . 39
8.4. Adjusting update settings . . . . . 39

How to . . . . . 41

9. Installation . . . . . 42
9.1. How do I install Bitdefender on a second computer? . . . . . 42
9.2. When should I reinstall Bitdefender? . . . . . 42
9.3. Where can I download my Bitdefender product from? . . . . . 43
9.4. How do I switch from one Bitdefender product to another? . . . . . 43
9.5. How do I use my Bitdefender license key after a Windows upgrade? . . . . . 44
9.6. How do I repair Bitdefender? . . . . . 46

10. Registration . . . . . 47
10.1. What Bitdefender product am I using? . . . . . 47
10.2. How do I register a trial version? . . . . . 47
10.3. When does my Bitdefender protection expire? . . . . . 47
10.4. How do I renew my Bitdefender protection? . . . . . 48

11. MyBitdefender . . . . . 49
11.1. How do I log in into MyBitdefender using another online account? . . . . . 49
11.2. How do I change the e-mail address used for MyBitdefender account? . . . . . 49
11.3. How do I reset the password for MyBitdefender account? . . . . . 50

12. Scanning with Bitdefender . . . . . 51
12.1. How do I scan a file or a folder? . . . . . 51
12.2. How do I scan my system? . . . . . 51
12.3. How do I create a custom scan task? . . . . . 51
12.4. How do I exclude a folder from being scanned? . . . . . 52
12.5. What to do when Bitdefender detected a clean file as infected? . . . . . 53
12.6. How do I check what viruses Bitdefender detected? . . . . . 53

13. Parental Control . . . . . 55
13.1. How do I protect my children from online threats? . . . . . 55
13.2. How do I restrict the Internet access for my child? . . . . . 55
13.3. How do I block my child's access to a website? . . . . . 56
13.4. How do I prevent my child from playing a game? . . . . . 57
13.5. How do I create Windows user accounts? . . . . . 57
13.6. How to remove a child profile . . . . . 58

14. Privacy Control . . . . . 60
14.1. How do I make sure my online transaction is secure? . . . . . 60
14.2. What can I do if my system has been stolen? . . . . . 60
14.3. How do I protect my Facebook account? . . . . . 61
14.4. How do I use file vaults? . . . . . 61
14.5. How do I remove a file permanently with Bitdefender? . . . . . 62

15. Tune Up . . . . . 63
15.1. How do I improve my system performance? . . . . . 63
15.1.1. Defragment your hard disk . . . . . 63
15.1.2. Clean-up your PC . . . . . 63
15.1.3. Clean Windows Registry . . . . . 64

15.1.4. Scan your system periodically . . . . . 64
16. Safebox Online Backup . . . . . 65
16.1. How do I access my backed up files from another computer? . . . . . 65
16.2. How can I share files with my friends? . . . . . 65
16.3. Where do I see the remaining space on my Safebox? . . . . . 65
16.4. How do I free space on my Safebox? . . . . . 66
17. Useful Information . . . . . 67
17.1. How do I test my antivirus solution? . . . . . 67
17.2. How do I remove Bitdefender? . . . . . 67
17.3. How do I keep my system protected after uninstalling Bitdefender? . . . . . 69
17.4. How do I automatically shut down the computer after the scan is over? . . . . . 69
17.5. How do I configure Bitdefender to use a proxy Internet connection? . . . . . 70
17.6. Am I using a 32 bit or a 64 bit version of Windows? . . . . . 71
17.7. How do I display hidden objects in Windows? . . . . . 72
17.8. How do I remove other security solutions? . . . . . 72
17.9. How do I use System Restore in Windows? . . . . . 73
17.10. How do I restart in Safe Mode? . . . . . 74
Managing your security . . . . . 75
18. Antivirus protection . . . . . 76
18.1. On-access scanning (real-time protection) . . . . . 77
18.1.1. Turning on or off real-time protection . . . . . 77
18.1.2. Adjusting the real-time protection level . . . . . 78
18.1.3. Configuring the real time protection settings . . . . . 78
18.1.4. Restoring the default settings . . . . . 81
18.2. On-demand scanning . . . . . 82
18.2.1. Autoscan . . . . . 82
18.2.2. Scanning a file or folder for malware . . . . . 82
18.2.3. Running a Quick Scan . . . . . 82
18.2.4. Running a System Scan . . . . . 83
18.2.5. Configuring a custom scan . . . . . 83
18.2.6. Antivirus Scan Wizard . . . . . 86
18.2.7. Checking scan logs . . . . . 89
18.3. Automatic scan of removable media . . . . . 89
18.3.1. How does it work? . . . . . 89
18.3.2. Managing removable media scan . . . . . 90
18.4. Configuring scan exclusions . . . . . 91
18.4.1. Excluding files or folders from scanning . . . . . 91
18.4.2. Excluding file extensions from scanning . . . . . 92
18.4.3. Managing scan exclusions . . . . . 92
18.5. Managing quarantined files . . . . . 93
18.6. Active Virus Control . . . . . 94
18.6.1. Checking detected applications . . . . . 94
18.6.2. Turning on or off Active Virus Control . . . . . 94
18.6.3. Adjusting the Active Virus Control protection . . . . . 95
18.6.4. Managing excluded processes . . . . . 95
18.7. Fixing system vulnerabilities . . . . . 96

18.7.1. Scanning your system for vulnerabilities . . . . . 96
18.7.2. Using automatic vulnerability monitoring . . . . . 97

19. Antispam . . . . . 100
19.1. Antispam insights . . . . . 100
19.1.1. Antispam filters . . . . . 100
19.1.2. Antispam operation . . . . . 101
19.1.3. Supported e-mail clients and protocols . . . . . 101
19.2. Turning on or off antispam protection . . . . . 102
19.3. Using the antispam toolbar in your mail client window . . . . . 102
19.3.1. Indicating detection errors . . . . . 103
19.3.2. Indicating undetected spam messages . . . . . 103
19.3.3. Configuring toolbar settings . . . . . 103
19.4. Configuring the Friends List . . . . . 104
19.5. Configuring the Spammers List . . . . . 105
19.6. Configuring the local antispam filters . . . . . 106
19.7. Configuring the cloud settings . . . . . 106

20. Privacy Control . . . . . 108
20.1. Antiphishing protection . . . . . 108
20.1.1. Bitdefender protection in the web browser . . . . . 110
20.1.2. Bitdefender alerts in the browser . . . . . 111
20.2. Chat encryption . . . . . 111
20.3. Data protection . . . . . 112
20.3.1. About data protection . . . . . 112
20.3.2. Configuring data protection . . . . . 112
20.3.3. Managing rules . . . . . 114
20.4. File encryption . . . . . 114
20.4.1. Managing file vaults from the Bitdefender interface . . . . . 114
20.4.2. Managing file vaults from Windows . . . . . 119
20.5. Deleting files permanently . . . . . 123

21. Firewall . . . . . 124
21.1. Turning on or off firewall protection . . . . . 125
21.2. Managing connection settings . . . . . 125
21.3. Managing firewall rules . . . . . 126
21.3.1. General rules . . . . . 126
21.3.2. Application rules . . . . . 127
21.3.3. Adapter rules . . . . . 130
21.4. Monitoring network activity . . . . . 131
21.5. Configuring alert intensity . . . . . 131
21.6. Configuring advanced settings . . . . . 132
21.6.1. Intrusion Detection System . . . . . 132
21.6.2. Other settings . . . . . 133

22. Safepay security for online transactions . . . . . 134
22.1. Using Bitdefender Safepay . . . . . 134
22.2. Configuring settings . . . . . 135
22.3. Managing bookmarks . . . . . 136
22.4. Hotspot protection for unsecured networks . . . . . 136

23. Wallet protection for your credentials ..... 138
23.1. Configuring the Wallet ..... 138
23.2. Turning on or off the Wallet protection ..... 140
23.3. Managing the Wallet settings ..... 140
24. Parental Control ..... 143
24.1. Accessing Parental Control dashboard ..... 143
24.2. Adding your child's profile ..... 144
24.2.1. Installing Parental Control on the Android device ..... 144
24.2.2. Monitoring the child's activity ..... 145
24.2.3. Configuring the General Settings ..... 146
24.3. Configuring Parental Control ..... 146
24.3.1. Web Control ..... 147
24.3.2. Applications Control ..... 149
24.3.3. Facebook protection ..... 149
24.3.4. Instant Messaging control ..... 150
24.3.5. Location ..... 151
24.3.6. Text messages control ..... 151
24.3.7. Phone numbers control ..... 152
25. Safego protection for Facebook ..... 153
26. Device Anti-Theft ..... 155
27. USB Immunizer ..... 157
28. Managing your computers remotely ..... 158
28.1. Accessing MyBitdefender ..... 158
28.2. Running tasks on the computers ..... 158
Tune-up and backup ..... 160
29. Tune-Up ..... 161
29.1. Cleaning up your PC ..... 161
29.2. Defragmenting hard disk volumes ..... 162
29.3. Finding duplicate files ..... 163
29.4. Cleaning Windows registry ..... 163
29.5. Recovering cleaned registry ..... 165
29.6. Performance Monitor ..... 165
30. Safebox online backup and sync ..... 167
30.1. Activating Safebox ..... 167
30.2. Managing Safebox from the Bitdefender window ..... 167
30.3. Managing Safebox from Windows ..... 168
30.3.1. Adding folders to Safebox ..... 169
30.3.2. Removing folders from Safebox ..... 169
30.3.3. Restoring files deleted from Safebox ..... 169
30.4. Managing Safebox from MyBitdefender ..... 170
30.5. Synchronizing files between your computers ..... 170
30.6. Upgrading your online space ..... 170
30.7. Removing files permanently ..... 171

30.8. Limit bandwidth allocation ..... 171

Troubleshooting ..... 172

31. Solving common issues ..... 173
31.1. My system appears to be slow ..... 173
31.2. Scan doesn't start ..... 175
31.3. I can no longer use an application ..... 176
31.4. I cannot connect to the Internet ..... 177
31.5. I cannot access a device on my network ..... 178
31.6. My Internet is slow ..... 180
31.7. How to update Bitdefender on a slow Internet connection ..... 181
31.8. My computer is not connected to the Internet. How do I update Bitdefender? ..... 181
31.9. Bitdefender services are not responding ..... 182
31.10. Antispam filter does not work properly ..... 182
31.10.1. Legitimate messages are marked as [spam] ..... 182
31.10.2. Many spam messages are not detected ..... 184
31.10.3. Antispam filter does not detect any spam message ..... 186
31.11. The Autofill feature in my Wallet doesn't work ..... 187
31.12. Bitdefender removal failed ..... 188
31.13. My system doesn't boot up after installing Bitdefender ..... 189

32. Removing malware from your system ..... 192
32.1. Bitdefender Rescue Mode ..... 192
32.2. What to do when Bitdefender finds viruses on your computer? ..... 194
32.3. How do I clean a virus in an archive? ..... 195
32.4. How do I clean a virus in an e-mail archive? ..... 196
32.5. What to do if I suspect a file as being dangerous? ..... 197
32.6. How to clean the infected files from System Volume Information ..... 197
32.7. What are the password-protected files in the scan log? ..... 198
32.8. What are the skipped items in the scan log? ..... 199
32.9. What are the over-compressed files in the scan log? ..... 199
32.10. Why did Bitdefender automatically delete an infected file? ..... 199

Contact us ..... 200

33. Asking for help ..... 201

34. Online resources ..... 203
34.1. Bitdefender Support Center ..... 203
34.2. Bitdefender Support Forum ..... 203
34.3. HOTforSecurity Portal ..... 204

35. Contact information ..... 205
35.1. Web addresses ..... 205
35.2. Local distributors ..... 205
35.3. Bitdefender offices ..... 205

Glossary ..... 208

# Installation

# 1. Preparing for installation

Before you install Bitdefender Total Security, complete these preparations to ensure the installation will go smoothly:

- Make sure that the computer where you plan to install Bitdefender meets the minimum system requirements. If the computer does not meet all the minimum system requirements, Bitdefender will not be installed or, if installed, it will not work properly and it will cause system slowdowns and instability. For a complete list of system requirements, please refer to "*System requirements*" (p. 3).
- Log on to the computer using an Administrator account.
- Remove any other similar software from the computer. Running two security programs simultaneously may affect their operation and cause major problems with the system. Windows Defender will be disabled during the installation.
- Disable or remove any firewall program that may be running on the computer. Running two firewall programs simultaneously may affect their operation and cause major problems with the system. Windows Firewall will be disabled during the installation.
- It is recommended that your computer be connected to the Internet during the installation, even when installing from a CD/DVD. If newer versions of the application files included in the installation package are available, Bitdefender can download and install them.

# 2. System requirements

You may install Bitdefender Total Security only on computers running the following operating systems:

- Windows XP with Service Pack 3 (32-bit)
- Windows Vista with Service Pack 2
- Windows 7 with Service Pack 1
- Windows 8

Before installation, make sure that your computer meets the minimum system requirements.

Note

To find out the Windows operating system your computer is running and hardware information, follow these steps:

- In **Windows XP**, **Windows Vista** and **Windows 7**, right-click **My Computer** on the desktop and then select **Properties** from the menu.
- In **Windows 8**, from the Windows Start screen, locate Computer (for example, you can start typing "Computer" directly in the Start screen) and then right-click its icon. Select Properties in the bottom menu. Look under System to see the system type.

## 2.1. Minimum system requirements

- 1 GB available free hard disk space (at least 800 MB on the system drive)
- 1.6 GHz processor
- 1 GB of memory (RAM) for Windows XP, Windows Vista, Windows 7 and Windows 8

## 2.2. Recommended system requirements

- 2 GB available free hard disk space (at least 800 MB on the system drive)
- Intel CORE Duo (2 GHz) or equivalent processor
- Memory (RAM):
  - 1 GB for Windows XP
  - 1.5 GB for Windows Vista, Windows 7 and Windows 8

## 2.3. Software requirements

To be able to use Bitdefender and all its features, your computer needs to meet the following software requirements:

- Internet Explorer 8 or higher
- Mozilla Firefox 3.6 or higher

- Chrome 20 or higher
- Yahoo! Messenger 9 or higher
- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express and Windows Mail (on 32-bit systems)
- Mozilla Thunderbird 3.0.4
- .NET Framework 3.5 (automatically installed with Bitdefender if missing)

# 3. Installing your Bitdefender product

You can install Bitdefender from the Bitdefender installation disc or using a web installer downloaded on your computer from the Bitdefender website or from other authorized websites (for example, the website of a Bitdefender partner or an online shop). You can download the installation file from the Bitdefender website at the following address: http://www.bitdefender.com/Downloads/.

If your purchase covers more than one computer (for example, you purchased Bitdefender Total Security for 3 PCs), repeat the installation process and register your product with the license key on every computer.

- To install Bitdefender from the installation disc, insert the disc in the optical drive. A welcome screen should be displayed in a few moments. Follow the instructions to start installation.

  Note

  The welcome screen provides an option to copy the installation package from the installation disc to a USB storage device. This is useful if you need to install Bitdefender on a computer that does not have a disc drive (for example, on a netbook). Insert the storage device into the USB drive and then click **Copy to USB**. Afterwards, go to the computer without a disc drive, insert the storage device into the USB drive and double-click `runsetup.exe` from the folder where you have saved the installation package.

  If the welcome screen does not appear, use Windows Explorer to browse to the disc's root directory and double-click the file `autorun.exe`.

- To install Bitdefender using the web installer downloaded on your computer, locate the file and double-click it.

## Validating the installation

Bitdefender will first check your system to validate the installation.

If your system does not meet the minimum requirements for installing Bitdefender, you will be informed of the areas that need improvement before you can proceed.

If an incompatible antivirus program or an older version of Bitdefender is detected, you will be prompted to remove it from your system. Please follow the directions to remove the software from your system, thus avoiding problems occurring later on. You may need to reboot your computer to complete the removal of detected antivirus programs.

The Bitdefender Total Security installation package is constantly updated. If you are installing from a CD/DVD, Bitdefender can download the newest versions of the files during the installation. Click **Yes** when prompted in order to allow Bitdefender

to download the files, ensuring you are installing the very latest version of the software.

Note
Downloading the installation files can take a long time, especially over slower Internet connections.

Once the installation is validated, the setup wizard will appear. Follow the steps to install Bitdefender Total Security.

## Step 1 - Welcome

The welcome screen lets you choose what type of installation you want to perform.

For a completely hassle-free installation experience, just click the **Install** button. Bitdefender will be installed in the default location with default settings and you will skip directly to Step 3 of the wizard.

If you wish to configure the installation settings, select **I want to customize my installation** and then click **Install** to move on to the next step.

Two additional tasks can be performed during this step:

- Please read the End User License Agreement before proceeding with the installation. The License Agreement contains the terms and conditions under which you may use Bitdefender Total Security.

  If you do not agree to these terms, close the window. The installation process will be abandoned and you will exit setup.

- Enable sending **Anonymous Usage Reports**. By enabling this option, reports containing information about how you use the product are sent to the Bitdefender servers. This information is essential for improving the product and can help us provide a better experience in the future. Please note that these reports contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.

## Step 2 - Customize installation settings

Note
This step appears only if you have chosen to customize the installation during the previous step.

The following options are available:

**Installation Path**

By default, Bitdefender Total Security will be installed in `C:\Program Files\Bitdefender\Bitdefender Total Security`. If you want to

change the installation path, click **Change** and select the folder in which you would like Bitdefender to be installed.

**Configure Proxy Settings**

Bitdefender Total Security requires access to the Internet for product registration, downloading security and product updates, in-cloud detection components, etc. If you use a proxy connection instead of a direct Internet connection, you must select this option and configure the proxy settings.

The settings can be imported from the default browser or you can enter them manually.

Click **Install with custom settings** to confirm your preferences and begin the installation. If you change your mind, click the corresponding **Nevermind, use default settings** button.

## Step 3 - Installation in progress

Wait for the installation to complete. Detailed information about the progress is displayed.

Critical areas on your system are scanned for viruses, the latest versions of the application files are downloaded and installed, and the Bitdefender services are started. This step can take a couple of minutes.

## Step 4 - Installation completed

A summary of the installation is displayed. If any active malware was detected and removed during the installation, a system reboot may be required.

You can either close the window, or continue with the initial setup of your software by clicking **Get started**.

## Step 5 - Register your product

Note

This step appears only if you have selected Get Started during the previous step.

To complete the registration of your product you need to enter a license key. An active Internet connection is required.

Proceed according to your situation:

- **I purchased the product**

  In this case, register the product by following these steps:

  1. Select **I purchased Bitdefender and I want to register now**.
  2. Type the license key in the corresponding field.

Note

You can find your license key:

- on the CD/DVD label.
- on the product registration card.
- in the online purchase e-mail.

3. Click **Register Now**.

- **I don't have a key, I want to try the product for free**

  In this case, you can use the product for a 30 day period. To begin the trial period, select **I don't have a key, I want to try the product for free**.

- Click **Next**.

## Step 6 - Configure product behavior

Bitdefender can be configured to automatically manage your security permanently or in certain situations. Use the switches to turn on or off **Autopilot** and **Automatic Game Mode**.

Enable the Autopilot for completely silent security. While on Autopilot, Bitdefender makes all security related decisions for you and you don't have to configure any settings. For more information, please refer to "*Autopilot*" (p. 15).

If you play your fair share of games, enable Automatic Game Mode and Bitdefender will detect when you launch a game and will enter Game Mode, modifying its settings so as to keep its impact on your system's performance to a minimum. For more information, please refer to "*Game Mode*" (p. 16).

Click **Next**.

## Step 7 - Login to MyBitdefender

A MyBitdefender account is required in order to use the online features of your product. For more information, please refer to "*MyBitdefender account*" (p. 35).

Proceed according to your situation.

**I want to create a MyBitdefender account**

To successfully create a MyBitdefender account, follow these steps:

1. Select **Create new account**.

   A new window will appear.

2. Type the required information in the corresponding fields. The data you provide here will remain confidential.

   - **E-mail** - enter your e-mail address.
   - **User name** - enter a user name for your account.

- **Password** - enter a password for your account. The password must be at least 6 characters long.
- **Confirm password** - retype the password.

Note

Once the account is created, you can use the provided e-mail address and password to log in to your account at https://my.bitdefender.com.

3. Click **Create**.
4. Before being able to use your account, you must complete the registration. Check your e-mail and follow the instructions in the confirmation e-mail sent by Bitdefender.

**I want to log in using my Microsoft, Facebook or Google account**

To log in with your Microsoft, Facebook or Google account, follow these steps:

1. Select the service you want to use. You will be redirected to the login page of that service.
2. Follow the instructions provided by the selected service to link your account to Bitdefender.

Note

Bitdefender does not get access to any confidential information such as the password of the account you use to log in, or the personal information of your friends and contacts.

**I already have a MyBitdefender account**

If you have logged in to an account from your product before, Bitdefender will detect it and prompt you to enter the password to log in to that account.

If you already have an active account, but Bitdefender does not detect it, or you simply want to log in with a different account, enter the e-mail address and password and click **Login to MyBitdefender**.

**Postpone for later**

If you want to leave this task for another time, click **Ask me later**. Remember that you must log in to an account to use the online features of the product.

# Getting started

# 4. The basics

Once you have installed Bitdefender Total Security, your computer is protected against all kinds of malware (such as viruses, spyware and trojans) and Internet threats (such as hackers, phishing and spam).

You can engage the Autopilot to enjoy completely silent security and you are not required to configure any settings. However, you may want to take advantage of the Bitdefender settings to fine-tune and improve your protection.

Bitdefender will make most security-related decisions for you and will rarely show pop-up alerts. Details about actions taken and information about program operation are available in the Events window. For more information, please refer to "*Events*" (p. 13).

From time to time, you should open Bitdefender and fix the existing issues. You may have to configure specific Bitdefender components or take preventive actions to protect your computer and your data.

If you have not registered the product, remember to do so until the trial period ends. For more information, please refer to "*Registering Bitdefender*" (p. 33).

To use the online features of Bitdefender Total Security, make sure to link your computer to a MyBitdefender account. For more information, please refer to "*MyBitdefender account*" (p. 35).

The "How to" (p. 41) section is where you will find step-by-step instructions on how to perform common tasks. If you experience issues while using Bitdefender, check the "*Solving common issues*" (p. 173) section for possible solutions to the most common problems.

## 4.1. Opening the Bitdefender window

To access the main interface of Bitdefender Total Security, follow the steps below:

- In **Windows XP**, **Windows Vista** and **Windows 7**:
  1. Click **Start** and go to **All Programs**.
  2. Click **Bitdefender**.
  3. Click **Bitdefender Total Security** or, quicker, double-click the Bitdefender icon in the system tray.
- In **Windows 8**:

  Locate Bitdefender Total Security from the Windows Start screen (for example, you can start typing "Bitdefender" directly in the Start screen) and then click its icon. Alternatively, open the Desktop app and then double-click the Bitdefender icon in the system tray.

For more information about the Bitdefender window and icon in the system tray, please refer to "*Bitdefender interface*" (p. 20).

## 4.2. Fixing issues

Bitdefender uses an issue tracking system to detect and inform you about the issues that may affect the security of your computer and data. By default, it will monitor only a series of issues that are considered to be very important. However, you can configure it as needed, choosing which specific issues you want to be notified about.

Detected issues include important protection settings that are turned off and other conditions that can represent a security risk. They are grouped into two categories:

- **Critical issues** - prevent Bitdefender from protecting you against malware or represent a major security risk.
- **Minor (non-critical) issues** - can affect your protection in the near future.

The Bitdefender icon in the system tray indicates pending issues by changing its color as follows:

**Red color:** Critical issues are affecting the security of your system. They require your immediate attention and must be fixed as soon as possible.
**Yellow color:** Non-critical issues are affecting the security of your system. You should check and fix them when you have the time.

Also, if you move the mouse cursor over the icon, a pop-up will confirm the existence of pending issues.

When you open the Bitdefender window, the Security status area on the upper toolbar will indicate the number and nature of issues affecting your system.

### 4.2.1. Fix All Issues wizard

To fix detected issues follow the **Fix All Issues** wizard.

1. To open the wizard, do any of the following:
   - Right-click the Bitdefender icon in the system tray and choose **View security issues**. Depending on the detected issues, the icon is either red (indicating critical issues) or yellow (indicating non-critical issues).
   - Open the Bitdefender window and click anywhere inside the Security status area on the upper toolbar (for example, you can click the **Fix All Issues** button).
2. You can see the issues affecting the security of your computer and data. All current issues are selected to be fixed.

If you do not want to fix a specific issue right away, clear the corresponding check box. You will be prompted to specify for how long to postpone fixing the issue. Choose the desired option from the menu and click **OK**. To stop monitoring the respective issue category, choose **Permanently**.

The issue status will change to **Postpone** and no action will be taken to fix the issue.

3. To fix the selected issues, click **Start**. Some issues are fixed immediately. For others, a wizard helps you fix them.

The issues that this wizard helps you fix can be grouped into these main categories:

- **Disabled security settings.** Such issues are fixed immediately, by enabling the respective security settings.
- **Preventive security tasks you need to perform.** When fixing such issues, a wizard helps you successfully complete the task.

### 4.2.2. Configuring status alerts

Bitdefender can inform you when issues are detected in the operation of the following program components:

- Firewall
- Antispam
- Antivirus
- Update
- Browser Security

You can configure the alert system to best serve your security needs by choosing which specific issues to be informed about. Follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **General**.
4. In the **General Settings** window, select the **Advanced** tab.
5. Click the **Configure status alerts** link.
6. Click the switches to turn on or off status alerts according to your preferences.

## 4.3. Events

Bitdefender keeps a detailed log of events concerning its activity on your computer. Whenever something relevant to the security of your system or data happens, a new message is added to the Bitdefender Events, in a similar way to a new e-mail appearing in your Inbox.

Events are a very important tool in monitoring and managing your Bitdefender protection. For instance, you can easily check if the update was successfully performed, if malware was found on your computer, etc. Additionally, you can take further action if needed or change actions taken by Bitdefender.

To access the Events log, follow these steps:

1. Open the Bitdefender window.
2. Click the **Events** on the upper toolbar to open the **Events Overview** window.

Messages are grouped according to the Bitdefender module whose activity they are related to:

- **Antivirus**
- **Firewall**
- **Update**
- **Safebox**
- **Privacy Control**
- **File Encryption**
- **Antispam**
- **Tune-Up**
- **Safego**

**Events counters** are displayed in the Bitdefender interface to allow easy identification of areas with outstanding events. These are icons appearing on specific modules that indicate the number of unread critical events related to a module's activity.

For example, if there is one unread critical event related to the activity of the Update module, the icon appears on the Update panel.

A counter showing the total number of unread messages from all modules appears on the Events button in the main window.

A list of events is available for each category. To find out information about a particular event in the list, click it. Event details are displayed in the lower part of the window. Each event comes with the following information: a short description, the action Bitdefender took on it when it happened, and the date and time when it occurred. Options may be provided to take further action if needed.

You can filter events by their importance and in the order they happened. There are three types of events filtered by their importance, each type indicated by a specific icon:

**Information** events indicate successful operations.

**Warning** events indicate non-critical issues. You should check and fix them when you have the time.

**Critical** events indicate critical issues. You should check them immediately.

To view the events that occurred in a period of time, select the desired period from the corresponding field.

To help you easily manage logged events, each section of the Events window provides options to delete or mark as read all events in that section.

## 4.4. Autopilot

For all the users who want nothing more from their security solution than to be protected without being bothered, Bitdefender Total Security has been designed with a built-in Autopilot mode.

While on Autopilot, Bitdefender applies an optimal security configuration and takes all security-related decisions for you. This means you will see no pop-ups, no alerts and you will not have to configure any settings whatsoever.

In Autopilot mode, Bitdefender automatically fixes critical issues, enables and quietly manages:

- Antivirus protection, provided by on-access scanning and continuous scanning.
- Firewall protection.
- Privacy protection, provided by antiphishing and antimalware filtering for your web browsing.
- Automatic updates.

To turn the Autopilot on or off, follow these steps:

1. Open the Bitdefender window.
2. Click the **User Mode** / **Autopilot** switch on the upper toolbar. When the switch is on the User Mode position, the Autopilot is off.

As long as the Autopilot is on, the Bitdefender icon in the system tray changes to .

Important
While the Autopilot is on, modifying any of the settings it manages will result in it being turned off.

To see a history of actions performed by Bitdefender while Autopilot was engaged, open the Events window.

## 4.5. Game Mode and Laptop Mode

Some computer activities, such as games or presentations, require increased system responsiveness and performance, and no interruptions. When your laptop is running on battery power, it is best that unnecessary operations, which consume additional power, be postponed until the laptop is connected back to A/C power.

To adapt to these particular situations, Bitdefender Total Security includes two special operation modes:

- Game Mode
- Laptop Mode

### 4.5.1. Game Mode

Game Mode temporarily modifies protection settings so as to minimize their impact on system performance. The following settings are applied when Game Mode is on:

- All Bitdefender alerts and pop-ups are disabled.
- On-access scanning is set to the **Permissive** protection level.
- Autoscan is turned off. Autoscan finds and uses time-slices when system resource usage falls below a certain threshold to perform recurring scans of the entire system.
- The Bitdefender firewall is set to normal mode (Paranoid mode is turned off). This means that all new connections (both incoming and outgoing) are automatically allowed, regardless of the port and protocol being used.
- Auto Update is turned off.
- Safebox Auto Sync is turned off.
- The Bitdefender toolbar in your web browser is disabled when you play browser-based online games.

While in Game Mode, the Bitdefender icon in the system tray changes to .

#### Using Game Mode

By default, Bitdefender automatically enters Game Mode when you start a game from the Bitdefender's list of known games or when an application goes to full screen. Bitdefender will automatically return to the normal operation mode when you close the game or when the detected application exits full screen.

If you want to manually turn on Game Mode, use one of the following methods:

- Right-click the Bitdefender icon in the system tray and select **Turn Game Mode On**.
- Enable using Game Mode keyboard shortcut. Press `Ctrl+Alt+Shift+G` (the default hotkey).

**Important**
Do not forget to turn Game Mode off when you finish. To do this, use the same methods you did when you turned it on.

## Turning on or off automatic Game Mode

To turn on or off automatic game mode, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **General**.
4. In the **General Settings** window, select the **General** tab.
5. Turn on or off automatic game mode by clicking the corresponding switch.

## Manually adding games to the Game list

If Bitdefender does not automatically enter Game Mode when you launch a certain game or application, you can manually add the application to the **Game list**. Once an application is added to the list, Bitdefender will operate in Game Mode as long as the application is in use.

To view and manage the Game list, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **General**.
4. In the **General Settings** window, select the **General** tab.
5. Click the **Game list** link.

Two buttons are available at the bottom of the list:

- **Add game** - add a new game or application to the Game list.

  A new window will appear. Browse to the application's executable file, select it and click **OK** to add it to the list.

- **Remove game** - remove a selected game or application from the list.

## Game Mode keyboard shortcut

To set and use a keyboard shortcut for entering / leaving Game Mode, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **General**.
4. In the **General Settings** window, select the **General** tab.
5. Make sure the Game Mode keyboard shortcut switch is on.
6. Set the desired combination:

a. The default combination is `Ctrl+Alt+Shift+G`.

   Modify the keys you want to use by checking one of the following: Control key (`Ctrl`), Shift key (`Shift`) or Alternate key (`Alt`).

b. In the edit field, type the letter corresponding to the regular key you want to use.

For example, if you want to use the `Ctrl+Alt+D` hotkey, you must check only `Ctrl` and `Alt` and type `D`.

Note
To disable the shortcut, turn off the **Game Mode keyboard shortcut** switch.

### 4.5.2. Laptop Mode

Laptop Mode is especially designed for laptop and notebook users. Its purpose is to minimize Bitdefender's impact on power consumption while these devices are running on battery. When Bitdefender operates in Laptop Mode, the Autoscan, Auto Update and Auto Sync features are turned off, as they require more system resources and, implicitly, increase power consumption.

Bitdefender detects when your laptop has switched to battery power and it automatically enters Laptop Mode. Likewise, Bitdefender automatically exits Laptop Mode, when it detects the laptop is no longer running on battery.

To turn on or off automatic laptop mode, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **General**.
4. In the **General Settings** window, select the **General** tab.
5. Turn on or off automatic laptop mode by clicking the corresponding switch.

If Bitdefender is not installed on a laptop, turn off automatic laptop mode.

## 4.6. Password-protecting Bitdefender settings

If you are not the only person with administrative rights using this computer, it is recommended that you protect your Bitdefender settings with a password.

To configure password protection for the Bitdefender settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **General**.

4. In the **General Settings** window, select the **General** tab.
5. Turn on password protection by clicking the switch.
6. Enter the password in the two fields and then click **OK**. The password must be at least 8 characters long.

Once you have set a password, anyone trying to change the Bitdefender settings will first have to provide the password.

Important

Be sure to remember your password or keep a record of it in a safe place. If you forget the password, you will have to reinstall the program or to contact Bitdefender for support.

To remove password protection, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **General**.
4. In the **General Settings** window, select the **General** tab.
5. Turn off password protection by clicking the switch. Enter the password and then click **OK**.

Note

To modify the password for your product, click the **Change password** link.

## 4.7. Anonymous usage reports

By default, Bitdefender sends reports containing information about how you use it to Bitdefender servers. This information is essential for improving the product and can help us offer you a better experience in the future. Please note that these reports will contain no confidential data, such as your name or IP address, and that they will not be used for commercial purposes.

In case you want to stop sending Anonymous usage reports, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **General**.
4. In the **General Settings** window, select the **Advanced** tab.
5. Click the switch to turn off Anonymous usage reports.

# 5. Bitdefender interface

Bitdefender Total Security meets the needs of computer beginners and very technical people alike. Its graphical user interface is designed to suit each and every category of users.

To see the status of the product and perform essential tasks, the Bitdefender system tray icon is available at any time.

The main window gives you access to important product information, the program modules and lets you perform common tasks. From the main window you can access the settings window for detailed configuration and advanced administrative tasks, and the Events window for an in-depth log of Bitdefender activity.

If you want to keep a constant eye on essential security information and have quick access to key settings, add the Security Widget to your desktop.

## 5.1. System tray icon

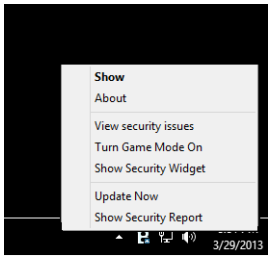
To manage the entire product more quickly, you can use the Bitdefender icon in the system tray.

**Note**
If you are using Windows Vista, Windows 7 or Windows 8, the Bitdefender icon may not be visible at all times. To make the icon appear permanently, follow these steps:

1. Click the arrow in the lower-right corner of the screen.
2. Click **Customize...** to open the Notification Area Icons window.
3. Select the option **Show icons and notifications** for the **Bitdefender Agent** icon.

If you double-click this icon, Bitdefender will open. Also, by right-clicking the icon, a contextual menu will allow you to quickly manage the Bitdefender product.

- **Show** - opens the main window of Bitdefender.
- **About** - opens a window where you can see information about Bitdefender and where to look for help in case something unexpected appears.
- **View security issues** - helps you remove current security vulnerabilities. If the option is unavailable, there are no issues to be fixed. For detailed information, please refer to "*Fixing issues*" (p. 12).
- **Turn Game Mode On / Off** - activates / deactivates Game Mode.



Tray Icon

- **Hide / Show Security Widget** - enables / disables Security Widget.
- **Update Now** - starts an immediate update. You can follow the update status in the Update panel of the main Bitdefender window.
- **Show Security Report** - opens a window where you can see a weekly status and recommendations for your system. You can follow the recommendations to improve your system security.

The Bitdefender system tray icon informs you when issues affect your computer or how the product operates, by displaying a special symbol, as follows:

Critical issues are affecting the security of your system. They require your immediate attention and must be fixed as soon as possible.

Non-critical issues are affecting the security of your system. You should check and fix them when you have the time.

The product operates in Game Mode.

Bitdefender Autopilot is engaged.

If Bitdefender is not working, the system tray icon appears on a gray background: . This usually happens when the license key expires. It can also occur when the Bitdefender services are not responding or when other errors affect the normal operation of Bitdefender.

## 5.2. Main window

The main Bitdefender window allows you to perform common tasks, quickly fix security issues, view information about events in product operation and configure product settings. Everything is just a few clicks away.

The window is organized in two main areas:

Upper toolbar
: This is where you can check your computer's security status and access important tasks.

Panels area
: This is where you can manage the main Bitdefender modules.

The MyBitdefender drop-down menu at the top of the window lets you manage your account and access the online features of your product from the account dashboard.

You can find several useful links on the lower part of the window. These links are also available in the Events and Settings windows.

| Link | Description |
|---|---|
| **Number of days left** | The time remaining before your current license expires is displayed. Click the link to open a window where you can see |

| Link | Description |
|---|---|
| | more information about your license key or register your product with a new license key. |
| **Help and Support** | Click this link if you need help with Bitdefender. A new window will appear where you can open the product help, go to the Support Center or contact support. |
| | Adds question marks in different areas of the Bitdefender window to help you easily find information about the different interface elements.<br>Move your mouse cursor over a mark to see quick information about the element next to it. |

### 5.2.1. Upper toolbar

The upper toolbar contains the following elements:

- **Security Status Area** on the left side of the toolbar, informs you if there are any issues affecting your computer's security and helps you fix them.

  The color of the security status area changes depending on the detected issues and different messages are displayed:

  - **The area is colored green.** There are no issues to fix. Your computer and data are protected.
  - **The area is colored yellow.** Non-critical issues are affecting the security of your system. You should check and fix them when you have the time.
  - **The area is colored red.** Critical issues are affecting the security of your system. You should address these issues immediately.

  By clicking **View Issues** in the center of the toolbar or anywhere in the security status area to its left, you can access a wizard that will help you easily remove any threats from your computer. For detailed information, please refer to "*Fixing issues*" (p. 12).

- **Events** allows you to access a detailed history of relevant events that occurred in the activity of the product. For detailed information, please refer to "*Events*" (p. 13).
- **Settings** allows you to access the settings window from where you can configure the product settings. For detailed information, please refer to "*Settings Overview window*" (p. 27).
- **Autopilot** / **User Mode** allows you to engage the Autopilot and enjoy completely silent security. For detailed information, please refer to "*Autopilot*" (p. 15).

## 5.2.2. Panels area

The panels area is where you can directly manage the Bitdefender modules.

To browse through the panels, use the slider below the panels area or the arrows located to the right and to the left.

Each module panel contains the following elements:

- The name of the module and a status message.
- An icon is available on the upper-right corner of most panels. Clicking it takes you directly to the advanced settings window.
- The icon of the module.

  If there are any events related to a module's activity that you have not read yet, an event counter will be displayed next to the module icon. For example, if there is one unread event related to the activity of the Update module, the icon appears on the Update panel. Click the counter to go directly to that module's Events window.
- A button that lets you perform important tasks related to the module.
- A switch is available on certain panels allowing you to turn on or off an important feature of the module.

You can organize the panels as you wish, by following these steps:

1. Click on the left side of the slider below the panels to open the Modules Overview window.
2. Drag individual module panels and drop them in other slots to rearrange the area according to your needs.
3. Click to return to the main window.

The panels available in this area are:

**Antivirus**

Antivirus protection is the foundation of your security. Bitdefender protects you in real-time and on-demand against all sorts of malware, such as viruses, trojans, spyware, adware, etc.

From the Antivirus panel you can easily access important scan tasks. Click **Scan Now** and select a task from the drop-down menu:

- Quick Scan
- System Scan
- Manage Scans
- Vulnerability Scan
- Rescue Mode

The **Autoscan** switch allows you to turn the Autoscan feature on or off.

For more information about scan tasks and how to configure antivirus protection, please refer to "*Antivirus protection*" (p. 76).

**Antispam**

The Bitdefender antispam module ensures your Inbox stays free of unwanted e-mails by filtering POP3 mail traffic.

Antispam protection is enabled by default.

You can click **Manage** in the Antispam panel and select Friends or Spammers from the drop-down menu to edit the corresponding address list.

For more information on configuring antispam protection, please refer to "*Antispam*" (p. 100).

**Privacy**

The privacy control module helps you keep important personal data private. It protects you while on the Internet against phishing attacks, fraud attempts, private data leaks, and more.

Click the **Secure** button on the Privacy Control panel and select **File Shredder** from the drop-down menu to start a wizard that will allow you to delete files permanently.

The Antiphishing switch allows you to turn on or off antiphishing protection.

For more information about how to configure Bitdefender to protect your privacy, please refer to "*Privacy Control*" (p. 108).

**Firewall**

The firewall protects you while you are connected to networks and the Internet by filtering all connection attempts.

By clicking **Manage Adapters** in the Firewall panel, you can configure general connection settings for network adapters.

The Firewall switch allows you to turn on or off firewall protection.

Warning

Because it exposes your computer to unauthorized connections, turning off the firewall should only be a temporary measure. Turn the firewall back on as soon as possible.

For more information about firewall configuration, please refer to "*Firewall*" (p. 124).

**Tune-Up**

Bitdefender Total Security offers not just security, it also helps you keep your computer's performance in shape.

Clicking **Optimize** in the Tune-Up panel lets you access a number of useful tools:

- PC Clean-Up
- Disk Defragmenter
- Duplicate Finder
- Registry Cleaner
- Registry Recovery

For more information about the performance optimization tools, please refer to "*Tune-Up*" (p. 161).

**Safebox**

Safebox lets you back up your important files to secure online servers, synchronize them between your devices and share them with your friends.

Clicking **Manage** allows you to select a task from the drop-down menu:

- **Manage folders** - add, remove and synchronize Safebox folders.
- **Manage shared files** - share files by uploading them to Safebox and creating links that can be accessed from anywhere.
- **Go to Dashboard** - manage your Safebox backups directly from the MyBitdefender dashboard in your web browser.

The Auto Sync switch allows you to turn on or off automatic synchronization for Safebox folders.

For more information, please refer to "*Safebox online backup and sync*" (p. 167).

**Update**

In a world where cyber criminals constantly try to come up with new ways to cause harm, it is essential to keep your security solution up to date if you are to stay one step ahead of them.

By default, Bitdefender automatically checks for updates every hour. If you want to turn off automatic updates, use the **Auto Update** switch on the Update panel.

Warning

This is a critical security issue. We recommend you to disable automatic update for as little time as possible. If Bitdefender is not updated regularly, it will not be able to protect you against the latest threats.

Click the **Update Now** button on the panel to start an immediate update.

For more information about configuring updates, please refer to "*Keeping Bitdefender up-to-date*" (p. 38).

**Safego**

To help you stay safe on social networks, you can access Safego, the Bitdefender security solution for social networks, directly from Bitdefender Total Security.

Click the **Manage** button on the Safego panel and select **Activate for Facebook** from the drop-down menu. If Safego has already been activated, you will be able to access statistics regarding its activity by selecting **View Reports for Facebook** in the menu.

For more information, please refer to "*Safego protection for Facebook*" (p. 153).

**File Encryption**

Create encrypted, password-protected logical drives (or vaults) on your computer where you can securely store your confidential and sensitive documents.

Click the **Encrypt** button on the File Encryption panel and select a task from the drop-down menu:

- **Add Files to Vault** - starts a wizard that will allow you to add your important files to a secure, encrypted file vault.
- **Remove Files from Vault** - starts a wizard that will allow you to remove files from a vault.
- **View Vault Files** - starts a wizard that will allow you to view the contents of a file vault.
- **Lock Vault** - starts a wizard that will allow you to lock a vault.

**Wallet**

Wallet is the password manager that helps you keep track of your passwords, protects your privacy and provides a secure browsing experience.

Click **Manage** button on the Wallet panel and select a task from the drop-down menu:

- **Open Wallet** - opens the existing Wallet database.
- **Export Wallet** - allows you to save the existing database to a location on your system.
- **Create new Wallet** - starts a wizard that will allow you to create a new Wallet database.

For more information about configuring Wallet, please refer to "*Wallet protection for your credentials*" (p. 138).

**Parental Control**

Bitdefender Parental Control allows you to restrict access to Internet and to specific applications, preventing your children from viewing inappropriate content whenever you are not around

Activate and click the **Configure** button on the Parental Control panel to start configuring your children's Windows accounts and monitor their activity wherever you are.

For more information about configuring Parental Control, please refer to "*Parental Control*" (p. 143).

## 5.3. Settings Overview window

The Settings Overview window gives you access to the advanced settings of your product. This is where you can configure Bitdefender in detail.

Select a module to configure its settings or perform security or administrative tasks. The following list briefly describes each module.

General
: Allows you to configure general product settings, such as the settings password, Game Mode, Laptop Mode, proxy settings and status alerts.

Antivirus
: Allows you to configure your protection against malware, detect and fix vulnerabilities of your system, set scan exclusions and manage quarantined files.

Antispam
: Allows you to keep your Inbox SPAM-free and to configure the antispam settings in detail.

Privacy Control
: Allows you to prevent data leaks and protect your privacy while you are online. Configure protection for your web browser, instant messaging software, create data protection rules, and more.

Firewall
: Allows you to configure general firewall settings, firewall rules, intrusion detection and monitor network activity.

Tune-Up
: Allows you to monitor your computer's performance and keep an eye on resource consumption.

Safebox
: Allows you to back up important data to secure online servers, synchronize files between your devices and share files with your friends.

Update
: Allows you to configure the update process in detail.

File Encryption
: Allows you to create and manage encrypted storage drives where you can keep sensitive data safe.

Wallet
Allows you to access your credentials with one master password.

To return to the main window, click on the upper-left corner of the window.

## 5.4. Security Widget

**Security Widget** is the quick and easy way to monitor and control Bitdefender Total Security. Adding this small and unintrusive widget to your desktop lets you see critical information and perform key tasks at all times:

- monitor scanning activity in real-time.
- monitor firewall activity in real-time.
- monitor the security status of your system and fix any existing issues.
- view notifications and get access to the latest events reported by Bitdefender.
- one click access to your MyBitdefender account.
- scan files or folders by dragging and dropping one or multiple items over the widget.

Security Widget

The overall security status of your computer is displayed **at the center** of the widget. The status is indicated by the color and shape of the icon that is displayed in this area.

Critical issues are affecting the security of your system.

They require your immediate attention and must be fixed as soon as possible. Click the status icon to begin fixing the reported issues.

Non-critical issues are affecting the security of your system. You should check and fix them when you have the time. Click the status icon to begin fixing the reported issues.

Your system is protected.

When an on-demand scan task is in progress, this animated icon is displayed.

When issues are reported, click the status icon to launch the Fix Issues wizard.

The button **on the left side** of the widget gives you direct access to the Firewall settings window, and also doubles up as a real-time graphical representation of firewall activity. When a blue bar appears on this button, it means the firewall module is actively filtering network connections. The taller the blue bar, the more intense is the activity of this module.

**The upper side** of the widget displays the unread events counter (the number of outstanding events reported by Bitdefender, if any). Click the event counter, for example for one unread event, to open the Events Overview window. For more information, please refer to "*Events*" (p. 13).

The button **on the right side** of the widget gives you direct access to the Antivirus settings window, and also doubles up as a real-time graphical representation of scanning activity. When a blue bar appears on this button, it indicates ongoing real-time antivirus scanning activity. The taller the blue bar, the more intense is the activity of this module.

The button **on the lower side** of the widget launches your MyBitdefender account control panel in a web browser window. For more information, please refer to "*MyBitdefender account*" (p. 35).

### 5.4.1. Scanning files and folders

You can use the Security Widget to quickly scan files and folders. Drag any file or folder you want to be scanned and drop it over the **Security Widget**.

The Antivirus Scan wizard will appear and guide you through the scanning process. The scanning options are pre-configured for the best detection results and can not be changed If infected files are detected, Bitdefender will try to disinfect them (remove the malware code). If disinfection fails, the Antivirus Scan wizard will allow you to specify other actions to be taken on infected files.

### 5.4.2. Hide / show Security Widget

When you no longer want to see the widget, click .

To restore Security Widget, use one of the following methods:

- From system tray:
  1. Right-click the Bitdefender icon in the system tray icon.
  2. Click **Show Security Widget** in the contextual menu that appears.
- From the Bitdefender interface:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **General**.
4. In the **General Settings** window, select the **General** tab.
5. Turn on **Display Security Widget** by clicking the corresponding switch.

## 5.5. Security Report

The Security Report provides a weekly status for your product and various tips to improve the system protection. These tips are important for managing the overall protection and you can easily see the actions you can take on your system.

The report is generated once a week and it summarizes the relevant information on your product activity so you can easily understand what occurred during this period of time.

The protection offered by the Security Report is divided into two categories:

- **Cloud protection** area - view information related to your system protection.
  - **File scan**

    Allows you to see the files scanned by Bitdefender for the week. You can see details, such as the number of scanned files, the number of infected files and the number of files cleaned by Bitdefender.

    For more information on the Antivirus protection, please refer to "*Antivirus protection*" (p. 76).
  - **Application scan**

    Allows you to see the number of blocked applications. To protect you against malicious applications, Bitdefender uses Active Virus Control to monitor the applications running on the system.

    For more information on Active Virus Control, please refer to "*Active Virus Control*" (p. 94).
  - **Web scan**

    Allows you to check the number of web pages scanned and blocked by Bitdefender. To protect you from disclosing personal information while browsing, Bitdefender secures your web traffic.
- **Privacy protection** area - view information related to your system privacy.
  - **Vulnerability scan**

    Allows you to see the number of vulnerabilities on your system.

For more information on the Vulnerability scan, please refer to "*Fixing system vulnerabilities*" (p. 96).

- **Safebox**

  Allows you to know how many files you have stored in your Safebox.

  For more information on Safebox, please refer to "*Safebox online backup and sync*" (p. 167).

- **File Encryption**

  Allows you to view how many files are secured against unwanted access.

  To find more information about how to create encrypted, password-protected logical drives (or vaults) on your computer, please refer to "*File encryption*" (p. 114).

### 5.5.1. Checking the Security Report

The Security Report uses an issue tracking system to detect and inform you about the issues that may affect the security of your computer and data. Detected issues include important protection settings that are turned off and other conditions that can represent a security risk. Using the report, you can configure specific Bitdefender components or take preventive actions to protect your computer and your private data.

To check the Security Report, follow these steps:

1. Access the report:
   - Open the Bitdefender window and click the icon at the top of the window.
   - Right-click the Bitdefender icon in the system tray and select **Show Security Report**.
   - Once a report is complete you will receive a pop-up notification. Click **Show** to access the security report.

     A web page will open on your web browser where you can view the generated report.
2. Take a look at the top of the window to see the overall security status.
3. Go with the mouse cursor over the selected areas to check our recommendations.
4. If there are issues you need to address, a little icon will appear.

   Move the mouse cursor over the icon for more information.
5. Follow the instructions to address the corresponding issues.

The color of the security status area changes depending on the detected issues and different messages are displayed:

- **The area is colored green.** There are no issues to fix. Your computer and data are protected.
- **The area is colored yellow.** Non-critical issues are affecting the security of your system. You should check and fix them when you have the time.
- **The area is colored red.** Critical issues are affecting the security of your system. You should address these issues immediately.

### 5.5.2. Turning on or off the Security Status notification

To turn on or off the Security Report notification, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **General**.
4. In the **General Settings** window, select the **General** tab.
5. Click the switch to turn on or off the Security Report notification.

   The Security Report notification is enabled by default.

# 6. Registering Bitdefender

In order to be protected by Bitdefender, you must register your product with a license key. The license key specifies how long you may use the product. As soon as the license key expires, Bitdefender stops performing its functions and protecting your computer.

You should purchase a license key or renew your license a few days before the current license key expires. For more information, please refer to "*Buying or renewing license keys*" (p. 33). If you are using a trial version of Bitdefender, you must register the product with a license key if you want to continue using it after the trial period ends.

## 6.1. Entering your license key

If, during the installation, you selected to evaluate the product, you can use it for a 30-day trial period. To continue using Bitdefender after the trial period expires, you must register the product with a license key.

A link that indicates the number of days left on your license appears at the bottom of the Bitdefender window. Click this link to open the registration window.

You can see the Bitdefender registration status, the current license key and how many days are left until the license expires.

To register Bitdefender Total Security:

1. Type the license key in the corresponding field.

Note

You can find your license key:

- on the CD label.
- on the product registration card.
- in the online purchase e-mail.

If you do not have a Bitdefender license key, click the link provided in the window to open a web page from where you can purchase one.

2. Click **Register Now**.

Even after you purchase a license key, until the in-product registration with the key is completed, Bitdefender Total Security will continue to appear as a trial version.

## 6.2. Buying or renewing license keys

If the trial period is going to end soon, you must purchase a license key and register your product. Similarly, if your current license key is going to expire soon, you must renew your license.

Bitdefender will alert you when the expiration date of your current license is approaching. Follow the instructions in the alert to purchase a new license.

You can visit a web page from where a license key can be purchased at any time, by following these steps:

1. Open the Bitdefender window.
2. Click the link that indicates the number of days left on your license, located at the bottom of the Bitdefender window, to open the product registration window.
3. Click **Don't have a license key? Buy one now!**
4. A web page will open on your web browser where you can purchase a Bitdefender license key.

# 7. MyBitdefender account

The online features of your product and additional Bitdefender services are available exclusively through MyBitdefender. You must link your computer to MyBitdefender by logging in to an account from Bitdefender Total Security in order to do any of the following:

- Recover your license key, should you ever lose it.
- Configure Parental Control settings for your children's Windows accounts and monitor their activity wherever you are.
- Back up and synchronize your important files to secure online servers using Safebox.
- Get protection for your Facebook account with Safego.
- Protect your computer and data against theft or loss with Anti-Theft.
- Manage Bitdefender Total Security remotely.

Multiple Bitdefender security solutions for PCs as well as other platforms integrate with MyBitdefender. You can manage the security of all the devices linked to your account from a single centralized dashboard.

Your MyBitdefender account can be accessed from any device connected to the Internet at https://my.bitdefender.com.

You can also access and manage your account directly from your product:

1. Open the Bitdefender window.
2. Click **MyBitdefender** at the top of the window and select an option from the drop-down menu:
   - **Account Settings**

     Log in to an account, create a new account, configure MyBitdefender behavior.
   - **Dashboard**

     Launch the MyBitdefender dashboard in your browser.
   - **Anti-Theft**

     Protect your computer and data against theft or loss.

## 7.1. Linking your computer to MyBitdefender

To link your computer to a MyBitdefender account, you must log in to an account from Bitdefender Total Security. Until you link your computer to MyBitdefender, you will be prompted to log in to MyBitdefender every time you want to use a feature that requires an account.

To open the MyBitdefender window from which you can create or log in to an account, follow these steps:

1. Open the Bitdefender window.
2. Click **MyBitdefender** at the top of the window and select **Account settings** from the drop-down menu.

If you have already logged in to an account, the account you are logged in to is displayed. Click **Go to MyBitdefender** to go to your dashboard. To change the account linked to the computer, click **Login with another account**.

If you have not logged in to an account, proceed according to your situation.

## I want to create a MyBitdefender account

To successfully create a MyBitdefender account, follow these steps:

1. Select **Create a new account**.

   A new window will appear.

2. Type the required information in the corresponding fields. The data you provide here will remain confidential.

   - **Email** - enter your e-mail address.
   - **User name** - enter a user name for your account.
   - **Password** - enter a password for your account. The password must be at least 6 characters long.
   - **Confirm password** - retype the password.

3. Click **Create**.
4. Before being able to use your account, you must complete the registration. Check your e-mail and follow the instructions in the confirmation e-mail sent by Bitdefender.

## I want to log in using my Microsoft, Facebook or Google account

To log in with your Microsoft, Facebook or Google account, follow these steps:

1. Click the icon of the service you want to use to log in. You will be redirected to the login page of that service.
2. Follow the instructions provided by the selected service to link your account to Bitdefender.

Note

Bitdefender does not get access to any confidential information such as the password of the account you use to log in, or the personal information of your friends and contacts.

## I already have a MyBitdefender account

If you already have an account but you have not logged in to it yet, follow these steps to log in:

1. Type the e-mail address and the password of your account in the corresponding fields.

Note
If you have forgotten your password, click **Forgot password** and follow the instructions to retrieve it.

2. Click **Login to MyBitdefender**.

Once the computer is linked to an account, you can use the provided e-mail address and password to log in at https://my.bitdefender.com.

You can also access your account directly from Bitdefender Total Security using the drop-down menu at the top of the window.

# 8. Keeping Bitdefender up-to-date

New malware is found and identified every day. This is why it is very important to keep Bitdefender up to date with the latest malware signatures.

If you are connected to the Internet through broadband or DSL, Bitdefender takes care of this itself. By default, it checks for updates when you turn on your computer and every **hour** after that. If an update is detected, it is automatically downloaded and installed on your computer.

The update process is performed on the fly, meaning that the files to be updated are replaced progressively. In this way, the update process will not affect product operation and, at the same time, any vulnerability will be excluded.

Important
To be protected against the latest threats keep Automatic Update turned on.

In some particular situations, your intervention is required in order to keep your Bitdefender protection up-to-date:

- If your computer connects to the Internet through a proxy server, you must configure the proxy settings as described in "*How do I configure Bitdefender to use a proxy Internet connection?*" (p. 70).
- If you do not have Internet connection, you can update Bitdefender manually as described in "*My computer is not connected to the Internet. How do I update Bitdefender?*" (p. 181). The manual update file is released once a week.
- Errors may occur while downloading updates on a slow Internet connection. To find out how to overcome such errors, please refer to "*How to update Bitdefender on a slow Internet connection*" (p. 181).
- If you are connected to the Internet through a dial-up connection, then it is recommended to regularly update Bitdefender by user request. For more information, please refer to "*Performing an update*" (p. 39).

## 8.1. Checking if Bitdefender is up-to-date

To check if your Bitdefender protection is up-to-date, follow these steps:

1. Open the Bitdefender window.
2. On the **Security Status Area**, on the left side of the toolbar, look for the time of the last update.

   This information will be displayed only if the security status is green.

For detailed information about the latest updates, check the update events:

1. In the main window, click **Events** on the upper toolbar.

2. In the **Events Overview** window, click **Update**.

You can find out when updates were initiated and information about them (whether they were successful or not, if they require a restart to complete the installation). If required, restart the system at your earliest convenience.

## 8.2. Performing an update

In order to perform updates, an Internet connection is required.

To start an update, do any of the following:

- Open the Bitdefender window and click **Update now** on the **Update** panel.
- Right-click the Bitdefender icon in the system tray and select **Update now**.

The Update module will connect to the Bitdefender update server and it will check for updates. If an update is detected, you will be asked to confirm it or the update will be performed automatically, depending on the update settings.

Important
It may be necessary to restart the computer when you have completed the update. We recommend doing it as soon as possible.

## 8.3. Turning on or off automatic update

To turn on or off automatic update, follow these steps:

1. Open the Bitdefender window.
2. On the **Update** panel, click the **Auto Update** switch.
3. A warning window will appear. You must confirm your choice by selecting from the menu how long you want the automatic update to be disabled. You can disable the automatic update for 5, 15 or 30 minutes, for an hour, permanently or until the system restart.

Warning
This is a critical security issue. We recommend you to disable automatic update for as little time as possible. If Bitdefender is not updated regularly, it will not be able to protect you against the latest threats.

## 8.4. Adjusting update settings

The updates can be performed from the local network, over the Internet, directly or through a proxy server. By default, Bitdefender will check for updates every hour, over the Internet, and install the available updates without alerting you.

The default update settings are suited for most users and you do not normally need to change them.

To adjust the update settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Update**.
4. In the **Update Settings** window, adjust the settings according to your preferences.

## Update location

Bitdefender is configured to update from the Bitdefender update servers on the Internet. The update location is a generic Internet address that is automatically redirected to the closest Bitdefender update server in your region.

Do not change the update location unless advised by a Bitdefender representative or by your network administrator (if you are connected to an office network).

You can switch back to the generic Internet update location by clicking **Default**.

## Update processing rules

You can choose between three ways to download and install updates:

- **Silent update** - Bitdefender automatically downloads and implements the update.
- **Prompt before downloading** - every time an update is available, you will be prompted before downloading it.
- **Prompt before installing** - every time an update was downloaded, you will be prompted before installing it.

Some updates require a restart to complete the installation. By default, if an update requires a restart, Bitdefender will keep working with the old files until the user voluntarily restarts the computer. This is to prevent the Bitdefender update process from interfering with the user's work.

If you want to be prompted when an update requires a restart, turn off the **Postpone reboot** option by clicking the corresponding switch.

# How to

# 9. Installation

## 9.1. How do I install Bitdefender on a second computer?

If you have purchased a license key for more than one computer, you can use the same license key to register a second PC.

To install Bitdefender correctly on a second computer, follow these steps:

1. Install Bitdefender from the CD/ DVD or using the installer provided in the online purchase e-mail and follow the same installation steps.

   At the beginning of the installation you will be prompted to download the latest installation files available.

2. When the registration window appears, enter the license key and click **Register Now**.

3. At the next step, you have the option to log in to your MyBitdefender account or create a new MyBitdefender account.

   You can also choose to create a MyBitdefender account later on.

4. Wait until the installation process is completed and close the window.

## 9.2. When should I reinstall Bitdefender?

In some situations, you may need to reinstall your Bitdefender product.

Typical situations when you would need to reinstall Bitdefender include the following:

- you have reinstalled the operating system.
- you have purchased a new computer.
- you want to change the display language of the Bitdefender interface.

To reinstall Bitdefender you can use the installation disc you purchased or download a new version from the Bitdefender website.

During the installation, you will be asked to register the product with your license key.

If you cannot find your license key, you can log in to https://my.bitdefender.com to retrieve it. Type the e-mail address and the password of your account in the corresponding fields.

For more information about the Bitdefender installation process, please refer to “*Installing your Bitdefender product*” (p. 5).

## 9.3. Where can I download my Bitdefender product from?

You can download your Bitdefender product from our authorized websites (for example, the website of a Bitdefender partner or an online shop) or from our website at the following address: http://www.bitdefender.com/Downloads/.

Note
Before running the kit, it is recommended to remove any antivirus solution installed on your system. When you use more than one security solution on the same computer, the system becomes unstable.

To install Bitdefender, follow these steps:

1. Double click the installer you have downloaded and follow the installation steps.
2. When the registration window appears, enter the license key and click **Register Now**.
3. At the next step, you have the option to log in to your MyBitdefender account or create a new MyBitdefender account.

   You can also choose to create a MyBitdefender account later on.
4. Wait until the installation process is completed and close the window.

## 9.4. How do I switch from one Bitdefender product to another?

You can easily switch from one Bitdefender product to another.

The three Bitdefender products you can install on your system are:

- Bitdefender Antivirus Plus
- Bitdefender Internet Security
- Bitdefender Total Security

If you do not have a license key for the product you want to use, follow these steps:

1. Open the Bitdefender window.
2. To access the product registration window, click the link that indicates the number of days left on your license, located at the bottom of the Bitdefender window.
3. Click **Don't have a license key? Buy one now!**
4. A web page will open on your web browser where you can purchase a Bitdefender license key.

After you buy the license key for the Bitdefender product you want to use, follow these steps:

1. Open the Bitdefender window.

2. A link that indicates the number of days left on your license appears at the bottom of the Bitdefender window.

   Click this link to open the registration window.

3. Enter the new license key and click **Register Now**.
4. You will be informed that the license key is for a different Bitdefender product.

   Click the corresponding link and follow the procedure to perform the installation.

## 9.5. How do I use my Bitdefender license key after a Windows upgrade?

This situation appears when you upgrade your operating system and you want to continue using your Bitdefender license key.

**If you are using Bitdefender 2009, 2010, 2011, 2012 or 2013 you can upgrade, free of charge, to the latest Bitdefender version, as follows:**

- From Bitdefender Antivirus 2009, 2010, 2011, 2012 or 2013 to the latest Bitdefender Antivirus Plus.
- From Bitdefender Internet Security 2009, 2010, 2011, 2012 or 2013 to the latest Bitdefender Internet Security.
- From Bitdefender Total Security 2009, 2010, 2011, 2012 or 2013 to the latest Bitdefender Total Security.

**There are 2 cases which may appear**:

- You have upgraded the operating system using the Windows Update and you notice Bitdefender is no longer working.

  In this case, you need to reinstall the product using the newest available version.

  To solve this situation, follow these steps:

  1. Remove Bitdefender by following these steps:
     - In **Windows XP**:
       a. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.
       b. Wait a few moments until the list of installed software is displayed.
       c. Find **Bitdefender** and select **Remove**.
       d. Click **Remove** and then **Reinstall/change my Bitdefender product**.
       e. Wait for the uninstall process to complete and then reboot your system.
     - In **Windows Vista** and **Windows 7**:

a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.

b. Wait a few moments until the installed software list is displayed.

c. Find **Bitdefender** and select **Uninstall**.

d. Click **Remove** and then **Reinstall/change my Bitdefender product**.

e. Wait for the uninstall process to complete and then reboot your system.

▶ In **Windows 8**:

a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.

b. Click **Uninstall a program** or **Programs and Features**.

c. Wait a few moments until the installed software list is displayed.

d. Find **Bitdefender** and select **Uninstall**.

e. Click **Remove** and then **Reinstall/change my Bitdefender product**.

f. Wait for the uninstall process to complete and then reboot your system.

2. Download the installation file by choosing the product you have a valid license key for.

   You can download the installation file from the Bitdefender website at the following address: http://www.bitdefender.com/Downloads/.

3. Double click the installer to start the installation process.

4. When the registration window appears, enter the license key and click **Register Now**.

5. At the next step, you have the option to log in to your **MyBitdefender** account or create a new **MyBitdefender** account.

   You can also choose to create a **MyBitdefender** account later on.

   Wait until the installation process is completed and close the window.

● You changed your system and you want to continue using the Bitdefender protection.

Therefore, you need to reinstall the product using the newest version.

To solve this situation, follow these steps:

1. Download the installation file by choosing the product you have a valid license key for.

   You can download the installation file from the Bitdefender website at the following address: http://www.bitdefender.com/Downloads/.

2. Double click the installer to start the installation process.
3. When the registration window appears, enter the license key and click **Register Now**.
4. At the next step, you have the option to log in to your **MyBitdefender** account or create a new **MyBitdefender** account.

   You can also choose to create a **MyBitdefender** account later on.

   Wait until the installation process is completed and close the window.

For more information about the Bitdefender installation process, please refer to "*Installing your Bitdefender product*" (p. 5).

## 9.6. How do I repair Bitdefender?

If you want to repair your Bitdefender Total Security from the Windows start menu, follow these steps:

- In **Windows XP**, **Windows Vista** and **Windows 7**:
  1. Click **Start** and go to **All Programs**.
  2. Click **Bitdefender Total Security**.
  3. Select **Repair** or **Uninstall**.

     A wizard will appear.
  4. Select **Repair**.

     This will take several minutes.
  5. You will need to restart the computer to complete the process.
- In **Windows 8**:
  1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
  2. Click **Uninstall a program** or **Programs and Features**.
  3. Select **Bitdefender Total Security** and click **Uninstall**.

     A wizard will appear.
  4. Select **Repair**.

     This will take several minutes.
  5. You will need to restart the computer to complete the process.

# 10. Registration

## 10.1. What Bitdefender product am I using?

To find out which Bitdefender program you have installed, follow these steps:

1. Open the Bitdefender window.
2. At the top of the window you should see one of the following:
   - Bitdefender Antivirus Plus
   - Bitdefender Internet Security
   - Bitdefender Total Security

## 10.2. How do I register a trial version?

If you have installed a trial version, you may only use it for a limited period of time. To continue using Bitdefender after the trial period expires, you must register your product with a license key.

To register Bitdefender, follow these steps:

1. Open the Bitdefender window.
2. A link that indicates the number of days left on your license appears at the bottom of the Bitdefender window.

   Click this link to open the registration window.
3. Enter the license key and click **Register Now**.

   If you do not have a license key, click the link provided in the window to visit a web page from where you can purchase one.
4. Wait until the registration process is completed and close the window.

## 10.3. When does my Bitdefender protection expire?

To find out the remaining number of days from your license key, follow these steps:

1. Open the Bitdefender window.
2. A link that indicates the number of days left on your license appears at the bottom of the Bitdefender window.
3. For additional information, click the link to open the registration window.
4. In the **Register Your Product** window, you can:
   - See the current license key
   - Register with another license key

- Purchase a license key

## 10.4. How do I renew my Bitdefender protection?

When your Bitdefender protection is about to expire, you must renew your license key.

- Follow these steps to visit a website where you can renew your Bitdefender license key:
  1. Open the Bitdefender window.
  2. A link that indicates the number of days left on your license appears at the bottom of the Bitdefender window. Click this link to open the registration window.
  3. Click **Don't have a license key? Buy one now!**
  4. A web page will open on your web browser where you can purchase a Bitdefender license key.

  Note
  As an alternative, you can contact the retailer you bought your Bitdefender product from.

- Follow these steps to register your Bitdefender with the new license key:
  1. Open the Bitdefender window.
  2. A link that indicates the number of days left on your license appears at the bottom of the Bitdefender window. Click this link to open the registration window.
  3. Enter the license key and click **Register Now**.
  4. Wait until the registration process is completed and close the window.

For more information, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 201).

# 11. MyBitdefender

## 11.1. How do I log in into MyBitdefender using another online account?

You have created a new MyBitdefender account and you want to use it from now on.

To successfully use another account, follow these steps:

1. Open the Bitdefender window.
2. Click **MyBitdefender** at the top of the window and select **Account Settings** from the drop-down menu.

   If you have already logged in to an account, the account you are logged in is displayed. Click **Login with another account** to change the account linked to the computer.

   A new window will appear.
3. Type the e-mail address and the password of your account in the corresponding fields.
4. Click **Login to MyBitdefender**
5. Click **Go to MyBitdefender** to go to your dashboard.

## 11.2. How do I change the e-mail address used for MyBitdefender account?

You have created a MyBitdefender account using an e-mail address you no longer use and now you would like to change it.

The e-mail address cannot be changed, but you can use a different e-mail address to create a new online account.

To successfully create another MyBitdefender account, follow these steps:

1. Open the Bitdefender window.
2. Click **MyBitdefender** at the top of the window and select **Account settings** from the drop-down menu.

   If you have already logged in to an account, the account you are logged in to is displayed. Click **Login with another account** to change the account linked to the computer.

   A new window will appear.
3. Select **Create a new account**.

4. Type in the required information in the corresponding fields. The data you provide here will remain confidential.
   - **E-mail** - enter your e-mail address.
   - **User name** - enter a user name for your account.
   - **Password** - enter a password for your account. The password must be at least 6 characters long.
   - **Confirm password** - retype the password.
   - Click **Create**.
5. Before being able to use your account, you must complete the registration. Check your e-mail and follow the instructions in the confirmation e-mail sent by Bitdefender.

Use the new e-mail address to log in to MyBitdefender.

## 11.3. How do I reset the password for MyBitdefender account?

To set a new password for your MyBitdefender account, follow these steps:

1. Open the Bitdefender window.
2. Click **MyBitdefender** at the top of the window and select **Account settings** from the drop-down menu.

   A new window will appear.
3. Click the **Forgot my password** link.
4. Type the e-mail address used to create your MyBitdefender account and click the **Recover password** link.
5. Check your e-mail and click the provided link.

   A new window will appear.
6. Type the new password. The password must be at least 6 characters long.
7. Retype the password in the **Confirm password** field.
8. Click **Submit** and then **Apply Changes**.

To access your MyBitdefender account, type your e-mail address and the new password you have just set.

# 12. Scanning with Bitdefender

## 12.1. How do I scan a file or a folder?

The easiest way to scan a file or folder is to right-click the object you want to scan, point to Bitdefender and select **Scan with Bitdefender** from the menu.

To complete the scan, follow the Antivirus Scan wizard. Bitdefender will automatically take the recommended actions on detected files.

If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

Typical situations when you would use this scanning method include the following:

- You suspect a specific file or folder to be infected.
- Whenever you download from the Internet files that you think they might be dangerous.
- Scan a network share before copying files to your computer.

## 12.2. How do I scan my system?

To perform a complete scan on the system, follow these steps:

1. Open the Bitdefender window.
2. On the **Antivirus** panel, click **Scan Now** and select **System Scan** from the drop-down menu.
3. Follow the Antivirus Scan wizard to complete the scan. Bitdefender will automatically take the recommended actions on detected files.

   If there remain unresolved threats, you will be prompted to choose the actions to be taken on them. For more information, please refer to "*Antivirus Scan Wizard*" (p. 86).

## 12.3. How do I create a custom scan task?

If you want to scan specific locations on your computer or to configure the scanning options, configure and run a customized scan task.

To create a customized scan task, proceed as follows:

1. Open the Bitdefender window.
2. On the **Antivirus** panel, click **Scan Now** and select **Manage Scans** from the drop-down menu.
3. Click **New custom task** to enter a name for the scan and select the locations to be scanned.

4. If you want to configure the scanning options in detail, select the **Advanced** tab.

   You can easily configure the scanning options by adjusting the scan level. Drag the slider along the scale to set the desired scan level.

   You can also choose to shutdown the computer when the scan is over if no threats are found. Remember that this will be the default behavior every time you run this task.

5. Click **OK** to save the changes and close the window.
6. Click **Schedule** if you want to set a schedule for your scan task.
7. Click **Start Scan** and follow the Antivirus Scan wizard to complete the scan. At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.
8. If you want to, you can quickly rerun a previous custom scan by clicking the corresponding entry in the available list.

## 12.4. How do I exclude a folder from being scanned?

Bitdefender allows excluding specific files, folders or file extensions from scanning.

Exclusions are to be used by users having advanced computer knowledge and only in the following situations:

- You have a large folder on your system where you keep movies and music.
- You have a large archive on your system where you keep different data.
- You keep a folder where you install different types of software and applications for testing purposes. Scanning the folder may result in losing some of the data.

To add the folder to the Exclusions list, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Exclusions** tab.
5. Make sure **Exclusions for files** is turned on by clicking the switch.
6. Click the **Excluded files and folders** link.
7. Click the **Add** button, located at the top of the exclusions table.
8. Click **Browse**, select the folder that you want to be excluded from scanning and then click **OK**.
9. Click **Add** and then **OK** to save the changes and close the window.

## 12.5. What to do when Bitdefender detected a clean file as infected?

There are cases when Bitdefender mistakenly flags a legitimate file as being a threat (a false positive). To correct this error, add the file to the Bitdefender Exclusions area:

1. Turn off the Bitdefender real-time antivirus protection:
   a. Open the Bitdefender window.
   b. Click the **Settings** button on the upper toolbar.
   c. In the **Settings Overview** window, select **Antivirus**.
   d. In the **Antivirus Settings** window, select the **Shield** tab.
   e. Click the switch to turn off **on-access scanning**.

      A warning window will appear. You must confirm your choice by selecting from the menu how long you want the real-time protection to be disabled. You can disable real-time protection for 5, 15 or 30 minutes, for an hour, permanently or until the system restart.
2. Display hidden objects in Windows. To find out how to do this, please refer to "*How do I display hidden objects in Windows?*" (p. 72).
3. Restore the file from the Quarantine area:
   a. Open the Bitdefender window.
   b. Click the **Settings** button on the upper toolbar.
   c. In the **Settings Overview** window, select **Antivirus**.
   d. In the **Antivirus Settings** window, select the **Quarantine** tab.
   e. Select the file and click **Restore**.
4. Add the file to the Exclusions list. To find out how to do this, please refer to "*How do I exclude a folder from being scanned?*" (p. 52).
5. Turn on the Bitdefender real-time antivirus protection.
6. Contact our support representatives so that we may remove the detection signature. To find out how to do this, please refer to "*Asking for help*" (p. 201).

## 12.6. How do I check what viruses Bitdefender detected?

Each time a scan is performed, a scan log is created and Bitdefender records the detected issues.

The scan log contains detailed information about the logged scanning process, such as scanning options, the scanning target, the threats found and the actions taken on these threats.

You can open the scan log directly from the scan wizard, once the scan is completed, by clicking **Show Log**.

To check a scan log or any detected infection at a later time, follow these steps:

1. Open the Bitdefender window.
2. Click the **Events** button on the upper toolbar.
3. In the **Events Overview** window, select **Antivirus**.
4. In the **Antivirus Events** window, select the **Virus Scan** tab.

   This is where you can find all malware scan events, including threats detected by on-access scanning, user-initiated scans and status changes for automatic scans.
5. In the events list, you can check what scans have been performed recently. Click an event to view details about it.
6. To open a scan log, click **View log**. The scan log will open in a new window.

# 13. Parental Control

## 13.1. How do I protect my children from online threats?

Bitdefender Parental Control allows you to restrict access to Internet and to specific applications, preventing your children from viewing inappropriate content whenever you are not around.

To configure the Parental Control, follow these steps:

1. Create limited (standard) Windows user accounts for your children to use. For more information, please refer to "*How do I create Windows user accounts?*" (p. 57).
2. Make sure you are logged on to the computer with an administrator account. Only users with administrative rights on the system (system administrators) can access and configure Parental Control.
3. Configure Parental Control for the Windows user accounts your children use.
   a. Open the Bitdefender window.
   b. Go to **Parental Control** panel and click the switch to turn it on.
   c. Click the **Configure** button.
   d. The Parental Control dashboard will open in a new window. This is where you can check and configure the Parental Control settings.
   e. Click **Add child** on the left-side menu.
   f. Enter the name and age of the child in the **Profile** tab. Setting the age of the child will automatically load settings considered appropriate for that age category, based on child development standards.

Check your children's activities and change the Parental Control settings using MyBitdefender from any computer or mobile device connected to the Internet.

For detailed information on using Parental Control, please refer to "*Parental Control*" (p. 143).

## 13.2. How do I restrict the Internet access for my child?

Once you have configured Parental Control, you can easily block Internet access for specific periods of time.

Bitdefender Parental Control enables you to control the Internet usage for your children even when you are not at home.

To restrict Internet access for certain times of day, follow these steps:

1. On any device with Internet access, open a web browser.

2. Go to: https://my.bitdefender.com
3. Log in to your account using your user name and password.
4. Click **Parental Control** to access the dashboard.
5. Select your child's profile on the left-side menu.
6. Click on the **Web** panel to access the **Web Activity** window.
7. Click **Schedule**.
8. Select from the grid the time intervals during which Internet access is blocked. You can click individual cells, or you can click and drag to cover longer periods. To start a new selection, click **Reset**.
9. Click the **Save** button.

Note
Bitdefender will perform updates every hour no matter if web access is blocked.

## 13.3. How do I block my child's access to a website?

Bitdefender Parental Control allows you to control the content accessed by your child while using the computer and enables you to block access to a website even when you are not at home.

To block access to a website, follow these steps:

1. On any device with Internet access, open a web browser.
2. Go to: https://my.bitdefender.com
3. Log in to your account using your user name and password.
4. Click **Parental Control** to access the dashboard.
5. Select your child's profile on the left-side menu.
6. Click on the **Web** panel to access the **Web Activity** window.
7. Click **Blacklist**.
8. Enter the website in the corresponding field.
9. Click **Add** to add the website to the list.
10. Select from the grid the time intervals during which access is allowed. You can click individual cells, or you can click and drag to cover longer periods.

    Click the **Save** button.
11. If you change your mind, select the website and click the corresponding **Remove** button.

## 13.4. How do I prevent my child from playing a game?

Bitdefender Parental Control allows you to control the content accessed by your child while using the computer.

If you need to restrict access to a game or an application, you can use Bitdefender Parental Control even when you are not at home.

To block access to a game, follow these steps:

1. On any device with Internet access, open a web browser.
2. Go to: https://my.bitdefender.com
3. Log in to your account using your user name and password.
4. Click **Parental Control** to access the dashboard.
5. Select your child's profile on the left-side menu.
6. Click on the **Applications** panel to access the **Applications Activity** window.
7. Click **Blacklist**.
8. Type (or copy and paste) the path to the executable in the corresponding field.
9. Click **Block** to add the application to the **Blocked apps**.
10. If you change your mind, click the corresponding **Allow** button.

## 13.5. How do I create Windows user accounts?

A Windows user account is a unique profile that includes all the settings, privileges and personal files for each user. Windows accounts let the home PC administrator control access for each user.

Setting up user accounts comes in handy when the PC is used by both parents and children – a parent can set up accounts for each child.

Choose which operating system you have to find out how to create Windows accounts.

- **Windows XP:**
  1. Log on to your computer as an administrator.
  2. Click Start, click Control Panel, and then click User Accounts.
  3. Click Create a new account.
  4. Type the name for the user. You can use the person's full name, first name, or a nickname. Then click Next.
  5. For the account type, choose Limited, and then Create Account. Limited accounts are appropriate for children because they cannot make system-wide changes or install certain applications.

6. Your new account will have been created and you will see it listed in the Manage Accounts screen.

- **Windows Vista or Windows 7:**

1. Log on to your computer as an administrator.
2. Click Start, click Control Panel, and then click User Accounts.
3. Click Create a new account.
4. Type the name for the user. You can use the person's full name, first name, or a nickname. Then click Next.
5. For the account type, click Standard, and then Create Account. Limited accounts are appropriate for children because they cannot make system-wide changes or install certain applications.
6. Your new account will have been created and you will see it listed in the Manage Accounts screen.

- **Windows 8:**

1. Log on to your computer as an administrator.
2. Point your mouse to the upper right corner of the screen, click Settings and then click Change PC settings.
3. Click Users in the left side menu and then click Add a user.

   You can create either a Microsoft account or a Local account. Read the description of each account type and follow the on-screen instructions to create a new account.

Note

Now that you have added new user accounts, you can create passwords for the accounts.

## 13.6. How to remove a child profile

If you want to remove an existent child profile, follow these steps:

1. On any device with Internet access, open a web browser.
2. Go to: https://my.bitdefender.com.
3. Log in to your account using your user name and password.
4. Click **Parental Control** to access the dashboard.
5. Select the child's profile you want to delete from the left-side menu.
6. Click **Account Settings**.
7. Click **Remove Profile**.

8. Click **OK**.

# 14. Privacy Control

## 14.1. How do I make sure my online transaction is secure?

To make sure your online operations remain private, you can use the browser provided by Bitdefender to protect your transactions and home banking applications.

Bitdefender Safepay is a secured browser designed to protect your credit card information, account number or any other sensitive data you may enter while accessing different online locations.

To keep your online activity secure and private, follow these steps:

1. Double-click the Bitdefender Safepay icon on your desktop.

   Bitdefender Safepay browser will appear.

2. Click the button to access the **Virtual Keyboard**.
3. Use the **Virtual Keyboard** when typing sensitive information such as your passwords.

## 14.2. What can I do if my system has been stolen?

Laptop theft is one of the main issues today affecting individuals and organizations throughout the world.

Bitdefender Anti-Theft allows you to not only locate and lock the stolen laptop, but also wipe all data to ensure that it will not be used by the thief.

To access the Anti-Theft features from your account, follow these steps:

1. Go to https://my.bitdefender.com and log in to your account.
2. Click **Anti-Theft**.
3. Select your computer from the list of devices.
4. Select the feature you want to use:

   - **Locate** - display your device's location on Google Maps.
   - **Wipe** - delete all data from your computer.

     Important
     After you wipe a device, all Anti-Theft features cease to function.

   - **Lock** - lock your computer and set a numeric PIN code for unlocking it.

## 14.3. How do I protect my Facebook account?

Safego is a Facebook application developed by Bitdefender to keep your social networking account safe.

Its role is to scan the links you receive from your Facebook friends and monitor your account privacy settings.

To access Safego from your Bitdefender product, follow these steps:

1. Open the Bitdefender window.
2. On the **Safego** panel, click **Manage** and select **Activate for Facebook** from the drop-down menu.

   You will be directed to your account.
3. Use your Facebook login information to connect to the Safego application.
4. Allow Safego access to your Facebook account.

## 14.4. How do I use file vaults?

The Bitdefender File Vault enables you to create encrypted, password-protected logical drives (or vaults) on your computer where you can securely store your confidential and sensitive documents. Physically, the vault is a file stored on the local hard drive having the .bvd extension.

When you create a file vault, two aspects are important: the size and the password. The default 50 MB size should be enough for your private documents, Excel files and other similar data. However, for videos or other large files you may need more space.

To securely store your confidential or sensitive files or folders in Bitdefender file vaults, follow these steps:

- **Create a file vault and set a strong password for it.**

  To create a vault, right-click an empty area of the desktop or in a folder on your computer, point to Bitdefender File Vault and select **Create vault**.

  A new window will appear. Proceed as follows:

  1. Click **Browse**, select the location of the vault and save the vault file under the desired name.
  2. Choose a drive letter from the menu. When you open the vault, a virtual disk drive labeled with the selected letter appears in **My Computer**.
  3. Type the vault password in the **Password** and **Confirm** fields.
  4. If you want to change the default size (50 MB) of the vault, type the desired value in the **Vault size** field.

5. Click Create if you only want to create the vault at the selected location. To create and display the vault as a virtual disk drive in **My Computer** click **Create and Open**.

Note

When you open the vault, a virtual disk drive appears in **My Computer**. The drive is labeled with the drive letter assigned to the vault.

- **Add the files or folders you want to keep safe to the vault.**

  In order to add a file to a vault, you must first open the vault.

  1. Browse to the .bvd vault file.
  2. Right-click the vault file, point to Bitdefender File Vault and select **Open**.
  3. In the window that appears, select a drive letter to assign to the vault, enter the password and click **Open**.

  You can now perform operations on the drive that corresponds to the desired file vault using Windows Explorer, just as you would with a regular drive. To add a file to an open vault, you can also right-click the file, point to Bitdefender File Vault and select **Add to file vault**.

- **Keep the vault locked at all times.**

  Only open vaults when you need to access them or manage their content. To lock a vault, right-click the corresponding virtual disk drive from **My Computer**, point to **Bitdefender File Vault** and select **Lock**.

- **Make sure not to delete the .bvd vault file.**

  Deleting the file also deletes the vault contents.

For more information about operating with file vaults, please refer to *"File encryption" (p. 114)*.

## 14.5. How do I remove a file permanently with Bitdefender?

If you want to remove a file permanently from your system, you need to delete the data physically from your hard disk.

The Bitdefender File Shredder will help you to quickly shred files or folders from your computer using the Windows contextual menu, by following these steps:

1. Right-click the file or folder you want to permanently delete, point to Bitdefender and select **File Shredder**.
2. A confirmation window will appear. Click **Yes** to start the File Shredder wizard.
3. Wait for Bitdefender to finish shredding the files.
4. The results are displayed. Click **Close** to exit the wizard.

# 15. Tune Up

## 15.1. How do I improve my system performance?

The system performance depends not only on the hardware configuration, such as the CPU load, memory usage and hard disk space. It is also directly connected to your software configuration and to your data management.

These are the main actions you can take with Bitdefender to improve your system's speed and performance:

- "*Defragment your hard disk*" (p. 63)
- "*Clean-up your PC*" (p. 63)
- "*Clean Windows Registry*" (p. 64)
- "*Scan your system periodically*" (p. 64)

### 15.1.1. Defragment your hard disk

It is recommended to defragment the hard disk in order to access files faster and improve overall system performance. The Disk Defragmenter helps you reduce file fragmentation and improves the performance of your system.

To start the Disk Defragmenter, follow these steps:

1. Open the Bitdefender window.
2. On the **Tune-Up** panel, click **Optimize** and select **Disk Defragmenter** from the drop-down menu.
3. Follow the wizard steps.

For more information about the Disk Defragmenter module, please refer to "*Defragmenting hard disk volumes*" (p. 162).

### 15.1.2. Clean-up your PC

The PC Clean-Up improves the system performance by removing those files which are no longer useful, such as: temporary Internet files, cookies and the system temporary files.

To start the PC Clean-Up, follow these steps:

1. Open the Bitdefender window.
2. On the **Tune-Up** panel, click **Optimize** and select **PC Clean-Up** from the drop-down menu.
3. Follow the wizard steps.

For more information about the PC Clean-UP module, please refer to "*Cleaning up your PC*" (p. 161).

### 15.1.3. Clean Windows Registry

Cleaning the Windows Registry can improve the performance of your system. To do this, use the Registry Cleaner. The Registry Cleaner scans the Windows Registry and deletes the invalid registry keys.

To start the Registry Cleaner, follow these steps:

1. Open the Bitdefender window.
2. On the **Tune-Up** panel, click **Optimize** and select **Registry Cleaner** from the drop-down menu.
3. Follow the wizard steps.

For more information about the Tune-UP module, please refer to "*Cleaning Windows registry*" (p. 163).

### 15.1.4. Scan your system periodically

Your system speed and its general behavior can also be affected by malware.

Make sure to scan your system periodically, at least once a week.

It is recommended to use the System Scan because it scans for all types of malware threatening the security of your system and it also scans inside archives.

To start the System Scan, follow these steps:

1. Open the Bitdefender window.
2. On the **Antivirus** panel, click **Scan now** and select **System Scan** from the drop-down menu.
3. Follow the wizard steps.

# 16. Safebox Online Backup

## 16.1. How do I access my backed up files from another computer?

With Bitdefender you can have access to the files you backed up with Safebox from any location, even when you are away from home.

All you need is a computer with Internet access and a web browser.

To access your files you need to log in to MyBitdefender:

1. On any device with Internet access, open a web browser.
2. Go to: https://my.bitdefender.com
3. Log in to your account using your user name and password.
4. Click **Safebox** to access the Safebox dashboard.

## 16.2. How can I share files with my friends?

Bitdefender Total Security is the solution that lets you share photos, music files, videos or documents with your friends.

To share a file with Bitdefender Total Security, choose one of the following:

1. Open the Bitdefender window.
2. On the **Safebox** panel, click **Manage** and select **Manage shared files** from the drop-down menu.
3. Drag the file and drop it in the **Manage Sharing** window.
4. Select the file and click **Share link**.
5. Click the provided link to copy the link to the clipboard.
6. To allow access to the shared file, send the link to the person you want to share the file with.

## 16.3. Where do I see the remaining space on my Safebox?

To find out the remaining space on your Safebox, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Safebox**.
4. In the **Quota used** section you can see the remaining space.

In case you have a large amount of data that includes music, movies or important files, the free online space may not be enough.

To upgrade your online space, click **Upgrade Safebox**.

The MyBitdefender page will open in your web browser. Follow the instructions to complete the purchase.

## 16.4. How do I free space on my Safebox?

Bitdefender offers you 2GB of free online space for your data.

In case you have a large amount of data that includes music, movies or important files, the free online space may not be enough.

To free space on your Safebox, follow these steps:

1. On any device with Internet access, open a web browser.
2. Go to: https://my.bitdefender.com
3. Log in to your account using your user name and password.
4. Click **Safebox** to access the Safebox dashboard.
5. Select the **Recycle Bin** tab.
6. Check the corresponding box to select the file you want to remove.
7. Click **Actions** and select **Remove** from the drop-down menu.
8. A confirmation window will appear. Click **OK** to acknowledge.

# 17. Useful Information

## 17.1. How do I test my antivirus solution?

To make sure that your Bitdefender product is properly running, we recommend you using the Eicar test.

The Eicar test allows you to check your antivirus protection using a safe file developed for this purpose.

To test your antivirus solution, follow these steps:

1. Download the test from the official webpage of the EICAR organization http://www.eicar.org/.
2. Click the **Anti-Malware Testfile** tab.
3. Click **Download** on the left-side menu.
4. From **Download area using the standard protocol http** click the **eicar.com** test file.
5. You will be informed that the page you are trying to access contains the EICAR-Test-File (not a virus).

   If you click **I understand the risks, take me there anyway**, the download of the test will begin and a Bitdefender pop-up will inform you that a virus was detected.

   Click **More details** to find out more information about this action.

If you do not receive any Bitdefender alert, we recommend you to contact Bitdefender for support as described in section *"Asking for help"* (p. 201).

## 17.2. How do I remove Bitdefender?

If you want to remove your Bitdefender Total Security, follow these steps:

- In **Windows XP**:
  1. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.
  2. Wait a few moments until the list of installed software is displayed.
  3. Find **Bitdefender** and select **Remove**.
  4. Click **Remove** and then **FULL uninstall of Bitdefender**.
  5. You have the following options:
     - **Uninstall and stay protected** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will be installed on your system to protect you against malware.

- **Uninstall without the app** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will not be installed.

Select the desired option and click **Next**.

6. Wait for the uninstall process to complete and then reboot your system.

- In **Windows Vista** and **Windows 7**:

1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
2. Wait a few moments until the installed software list is displayed.
3. Find **Bitdefender** and select **Uninstall**.
4. Click **Uninstall** and then **FULL uninstall of Bitdefender**.
5. You have the following options:

   - **Uninstall and stay protected** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will be installed on your system to protect you against malware.
   - **Uninstall without the app** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will not be installed.

   Select the desired option and click **Next**.

6. Wait for the uninstall process to complete and then reboot your system.

- In **Windows 8**:

1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
2. Click **Uninstall a program** or **Programs and Features**.
3. Select **Bitdefender Total Security** and click **Uninstall**.
4. Click **Uninstall** and then **FULL uninstall of Bitdefender**.
5. You have the following options:

   - **Uninstall and stay protected** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will be installed on your system to protect you against malware.
   - **Uninstall without the app** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will not be installed.

   Select the desired option and click **Next**.

6. Wait for the uninstall process to complete and then reboot your system.

Note

Bitdefender 60-Second Virus Scanner is a free application which uses in-the-cloud scanning technology to detect malicious programs and threats in less than 60 seconds.

## 17.3. How do I keep my system protected after uninstalling Bitdefender?

During the Bitdefender Total Security removal process, you have the option to **Uninstall and stay protected**. If you select this option, Bitdefender 60-Second Virus Scanner will be installed on your system.

Bitdefender 60-Second Virus Scanner is a free application which uses in-the-cloud scanning technology to detect malicious programs and threats in less than 60 seconds.

You can continue using the application even if you reinstall Bitdefender or you install any other antivirus program on your system.

If you want to remove Bitdefender 60-Second Virus Scanner, follow these steps:

- In **Windows XP**:
  1. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.
  2. Wait a few moments until the list of installed software is displayed.
  3. Find **Bitdefender 60-Second Virus Scanner** and select **Remove**.
  4. Select **Uninstall** at the next step and wait for the process to finish.
- In **Windows Vista** and **Windows 7**:
  1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  2. Wait a few moments until the installed software list is displayed.
  3. Find **Bitdefender 60-Second Virus Scanner** and select **Uninstall**.
  4. Select **Uninstall** at the next step and wait for the process to finish.
- In **Windows 8**:
  1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
  2. Click **Uninstall a program** or **Programs and Features**.
  3. Select **Bitdefender 60-Second Virus Scanner** and click **Uninstall**.
  4. Select **Uninstall** at the next step and wait for the process to finish.

## 17.4. How do I automatically shut down the computer after the scan is over?

Bitdefender offers multiple scan tasks that you can use to make sure your system is not infected with malware. Scanning the entire computer may take longer time to complete depending on your system's hardware and software configuration.

For this reason, Bitdefender allows you to configure Bitdefender to shut down your system as soon as the scan is over.

Consider this example: you have finished your work at the computer and you want to go to sleep. You would like to have your entire system checked for malware by Bitdefender.

This is how you set up Bitdefender to shut down your system at the end of the scan:

1. Open the Bitdefender window.
2. On the **Antivirus** panel, click **Scan Now** and select **Manage Scans** from the drop-down menu.
3. Click **New custom task** to enter a name for the scan and select the locations to be scanned.
4. If you want to configure the scanning options in detail, select the **Advanced** tab.
5. Click **OK** to save the changes and close the window.
6. Choose to shutdown the computer when the scan is over if no threats are found.
7. Click **Start Scan**.

If no threats are found, the computer will shut down.

If there remain unresolved threats, you will be prompted to choose the actions to be taken on them. For more information, please refer to *"Antivirus Scan Wizard" (p. 86)*.

## 17.5. How do I configure Bitdefender to use a proxy Internet connection?

If your computer connects to the Internet through a proxy server, you must configure Bitdefender with the proxy settings. Normally, Bitdefender automatically detects and imports the proxy settings from your system.

Important

Home Internet connections do not normally use a proxy server. As a rule of thumb, check and configure the proxy connection settings of your Bitdefender program when updates are not working. If Bitdefender can update, then it is properly configured to connect to the Internet.

To manage the proxy settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **General**.
4. In the **General Settings** window, select the **Advanced** tab.

5. Turn on proxy usage by clicking the switch.
6. Click the **Manage proxies** link.
7. There are two options to set the proxy settings:
   - **Import proxy settings from default browser** - proxy settings of the current user, extracted from the default browser. If the proxy server requires a username and a password, you must specify them in the corresponding fields.

     Note
     Bitdefender can import proxy settings from the most popular browsers, including the latest versions of Internet Explorer, Mozilla Firefox and Opera.

   - **Custom proxy settings** - proxy settings that you can configure yourself. The following settings must be specified:
     - **Address** - type in the IP of the proxy server.
     - **Port** - type in the port Bitdefender uses to connect to the proxy server.
     - **User name** - type in a user name recognized by the proxy.
     - **Password** - type in the valid password of the previously specified user.
8. Click **OK** to save the changes and close the window.

Bitdefender will use the available proxy settings until it manages to connect to the Internet.

## 17.6. Am I using a 32 bit or a 64 bit version of Windows?

To find out if you have a 32 bit or a 64 bit operating system, follow these steps:

- In **Windows XP**:
  1. Click **Start**.
  2. Locate **My Computer** on the **Start** menu.
  3. Right-click **My Computer** and select **Properties**.
  4. If you see **x64 Edition** listed under **System**, you are running the 64 bit version of Windows XP.

     If you do not see **x64 Edition** listed, you are running a 32 bit version of Windows XP.
- In **Windows Vista** and **Windows 7**:
  1. Click **Start**.
  2. Locate **Computer** on the **Start** menu.
  3. Right-click **Computer** and select **Properties**.
  4. Look under **System** in order to check the information about your system.

- In **Windows 8**:
  1. From the Windows Start screen, locate **Computer** (for example, you can start typing "Computer" directly in the Start screen) and then right-click its icon.
  2. Select **Properties** in the bottom menu.
  3. Look under **System** to see the system type.

## 17.7. How do I display hidden objects in Windows?

These steps are useful in those cases where you are dealing with a malware situation and you need to find and remove the infected files, which could be hidden.

Follow these steps to display hidden objects in Windows:

1. Click **Start**, go to **Control Panel**.

   In **Windows 8**: From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
2. Select **Folder Options**.
3. Go to **View** tab.
4. Select **Display contents of system folders** (for Windows XP only).
5. Select **Show hidden files and folders**.
6. Clear **Hide extensions for known file types**.
7. Clear **Hide protected operating system files**.
8. Click **Apply** and then **OK**.

## 17.8. How do I remove other security solutions?

The main reason for using a security solution is to provide protection and safety for your data. But what happens when you have more than one security product on the same system?

When you use more than one security solution on the same computer, the system becomes unstable. The Bitdefender Total Security installer automatically detects other security programs and offers you the option to uninstall them.

If you did not remove the other security solutions during the initial installation, follow these steps:

- In **Windows XP**:
  1. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.
  2. Wait a few moments until the list of installed software is displayed.
  3. Find the name of the program you want to remove and select **Remove**.

4. Wait for the uninstall process to complete and then reboot your system.

- In **Windows Vista** and **Windows 7**:
  1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  2. Wait a few moments until the installed software list is displayed.
  3. Find the name of the program you want to remove and select **Uninstall**.
  4. Wait for the uninstall process to complete and then reboot your system.
- In **Windows 8**:
  1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
  2. Click **Uninstall a program** or **Programs and Features**.
  3. Wait a few moments until the installed software list is displayed.
  4. Find the name of the program you want to remove and select **Uninstall**.
  5. Wait for the uninstall process to complete and then reboot your system.

If you fail to remove the other security solution from your system, get the uninstall tool from the vendor website or contact them directly in order to provide you with the uninstall guidelines.

## 17.9. How do I use System Restore in Windows?

If you cannot start the computer in normal mode, you can boot up in Safe Mode and use System Restore to restore to a time when you could start the computer without errors.

To perform the System Restore, you must be logged on to Windows as an administrator.

To use System Restore, follow these steps:

- In **Windows XP**:
  1. Log on to Windows in Safe Mode.
  2. Follow the path from the Windows start menu: **Start → All Programs → System Tools → System Restore**.
  3. On the **Welcome to System Restore** page, click to select the **Restore my computer to an earlier time** option, and then click Next.
  4. Follow the wizard steps and you should be able to boot up the system in normal mode.
- In **Windows Vista** and **Windows 7**:
  1. Log on to Windows in Safe Mode.

2. Follow the path from the Windows start menu: **All Programs** → **Accessories** → **System Tools** → **System Restore**.
3. Follow the wizard steps and you should be able to boot up the system in normal mode.

- In **Windows 8**:
  1. Log on to Windows in Safe Mode.
  2. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
  3. Select **Recovery** and then **Open System Restore**.
  4. Follow the wizard steps and you should be able to boot up the system in normal mode.

## 17.10. How do I restart in Safe Mode?

Safe mode is a diagnostic operating mode, used mainly to troubleshoot problems affecting normal operation of Windows. Such problems range from conflicting drivers to viruses preventing Windows from starting normally. In Safe Mode only a few applications work and Windows loads just the basic drivers and a minimum of operating system components. This is why most viruses are inactive when using Windows in Safe Mode and they can be easily removed.

To start Windows in Safe Mode:

1. Restart the computer.
2. Press the **F8** key several times before Windows starts in order to access the boot menu.
3. Select **Safe Mode** in the boot menu or **Safe Mode with Networking** if you want to have Internet access.
4. Press **Enter** and wait while Windows loads in Safe Mode.
5. This process ends with a confirmation message. Click **OK** to acknowledge.
6. To start Windows normally, simply reboot the system.

# Managing your security

# 18. Antivirus protection

Bitdefender protects your computer from all kinds of malware (viruses, Trojans, spyware, rootkits and so on). The protection Bitdefender offers is divided into two categories:

- On-access scanning - prevents new malware threats from entering your system. Bitdefender will, for example, scan a word document for known threats when you open it, and an e-mail message when you receive one.

  On-access scanning ensures real-time protection against malware, being an essential component of any computer security program.

  Important
  To prevent viruses from infecting your computer keep **on-access scanning** enabled.

- On-demand scanning - allows detecting and removing the malware that already resides in the system. This is the classic scan initiated by the user - you choose what drive, folder or file Bitdefender should scan, and Bitdefender scans it - on-demand.

  With Autoscan turned on, there is hardly any need to manually run scans for malware. Autoscan will scan your computer over and over again, taking appropriate actions when malware is detected. Autoscan runs only when enough system resources are available so as not to slow down the computer.

Bitdefender automatically scans any removable media that is connected to the computer to make sure it can be safely accessed. For more information, please refer to *"Automatic scan of removable media" (p. 89)*.

Advanced users can configure scan exclusions if they do not want specific files or file types to be scanned. For more information, please refer to *"Configuring scan exclusions" (p. 91)*.

When it detects a virus or other malware, Bitdefender will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection. Files that cannot be disinfected are moved to quarantine in order to contain the infection. For more information, please refer to *"Managing quarantined files" (p. 93)*.

If your computer has been infected with malware, please refer to *"Removing malware from your system" (p. 192)*. To help you clean your computer of malware that cannot be removed from within the Windows operating system, Bitdefender provides you with Rescue Mode. This is a trusted environment, especially designed for malware removal, which enables you to boot your computer independent of Windows. When the computer runs in Rescue Mode, Windows malware is inactive, making it easy to remove.

To protect you against unknown malicious applications, Bitdefender uses Active Virus Control, an advanced heuristic technology, which continuously monitors the applications running on your system. Active Virus Control automatically blocks applications that exhibit malware-like behavior to stop them from damaging your computer. Occasionally, legitimate applications may be blocked. In such situations, you can configure Active Virus Control not to block those applications again by creating exclusion rules. To learn more, please refer to "*Active Virus Control*" (p. 94).

Many forms of malware are designed to infect systems by exploiting their vulnerabilities, such as missing operating system updates or outdated applications. Bitdefender helps you easily identify and fix system vulnerabilities in order to make your computer more secure against malware and hackers. For more information, please refer to "*Fixing system vulnerabilities*" (p. 96).

## 18.1. On-access scanning (real-time protection)

Bitdefender provides continuous, real-time protection against a wide range of malware threats by scanning all accessed files, e-mail messages and the communications through Instant Messaging Software applications (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

The default real-time protection settings ensure good protection against malware, with minor impact on system performance. You can easily change the real-time protection settings according to your needs by switching to one of the predefined protection levels. Or, if you are an advanced user, you can configure the scan settings in detail by creating a custom protection level.

### 18.1.1. Turning on or off real-time protection

To turn on or off real-time protection against malware, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Shield** tab.
5. Click the switch to turn on or off On-access scanning.
6. If you want to disable real-time protection, a warning window will appear. You must confirm your choice by selecting from the menu how long you want the real-time protection to be disabled. You can disable real-time protection for 5, 15 or 30 minutes, for an hour, permanently or until the system restart. The real-time protection will automatically turn on when the selected time will expire.

Warning
This is a critical security issue. We recommend you to disable real-time protection for as little time as possible. If real-time protection is disabled, you will not be protected against malware threats.

### 18.1.2. Adjusting the real-time protection level

The real-time protection level defines the scan settings for real-time protection. You can easily change the real-time protection settings according to your needs by switching to one of the predefined protection levels.

To adjust the real-time protection level, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Shield** tab.
5. Drag the slider along the scale to set the desired protection level. Use the description on the right side of the scale to choose the protection level that better fits your security needs.

### 18.1.3. Configuring the real time protection settings

Advanced users might want to take advantage of the scan settings Bitdefender offers. You can configure the real-time protection settings in detail by creating a custom protection level.

To configure the real time protection settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Shield** tab.
5. Click **Custom**.
6. Configure the scan settings as needed.
7. Click **OK** to save the changes and close the window.

#### Information on the scan options

You may find this information useful:

- If you are not familiar with some of the terms, check them in the glossary. You can also find useful information by searching the Internet.

- **Scan options for accessed files.** You can set Bitdefender to scan all accessed files or applications (program files) only. Scanning all accessed files provides best protection, while scanning applications only can be used for better system performance.

  By default, both local folders and network shares are subject to on-access scanning. For better system performance, you can exclude network locations from on-access scanning.

  Applications (or program files) are far more vulnerable to malware attacks than other types of files. This category includes the following file extensions:

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Scan inside archives.** Scanning inside archives is a slow and resource-intensive process, which is therefore not recommended for real-time protection. Archives containing infected files are not an immediate threat to the security of your system. The malware can affect your system only if the infected file is extracted from the archive and executed without having real-time protection enabled.

  If you decide on using this option, you can set a maximum accepted size limit of archives to be scanned on-access. Select the corresponding check box and type the maximum archive size (in MB).

- **Scan options for e-mail, web and instant messaging traffic.** To prevent malware from being downloaded to your computer, Bitdefender automatically scans the following malware entry points:
  - ▶ incoming and outgoing e-mails
  - ▶ web traffic
  - ▶ files received via Yahoo! Messenger

  Scanning the web traffic may slow down web browsing a little, but it will block malware coming from the Internet, including drive-by downloads.

Though not recommended, you can disable e-mail, web or instant messaging antivirus scan to increase system performance. If you disable the corresponding scan options, the e-mails and files received or downloaded from the Internet will not be scanned, thus allowing infected files to be saved to your computer. This is not a major threat because real-time protection will block the malware when the infected files are accessed (opened, moved, copied or executed).

- **Scan boot sectors.** You can set Bitdefender to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.
- **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Scan for keyloggers.** Select this option to scan your system for keylogger applications. Keyloggers record what you type on your keyboard and send reports over the Internet to a malicious person (hacker). The hacker can find out sensitive information from the stolen data, such as bank account numbers and passwords, and use it to gain personal benefits.

## Actions taken on detected malware

You can configure the actions taken by the real-time protection.

To configure the actions, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Shield** tab.
5. Click **Custom**.
6. Configure the scan settings as needed.
7. Click **OK** to save the changes and close the window.

The following actions can be taken by the real time protection in Bitdefender:

**Take proper actions**

Bitdefender will take the recommended actions depending on the type of detected file:

- **Infected files.** Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Bitdefender will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection.

Files that cannot be disinfected are moved to quarantine in order to contain the infection. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, please refer to "*Managing quarantined files*" (p. 93).

Important

For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

- **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available. They will be moved to quarantine to prevent a potential infection.

  By default, quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

- **Archives containing infected files.**
  - Archives that contain only infected files are deleted automatically.
  - If an archive contains both infected and clean files, Bitdefender will attempt to delete the infected files provided it can reconstruct the archive with the clean files. If archive reconstruction is not possible, you will be informed that no action can be taken so as to avoid losing clean files.

**Move files to quarantine**

Moves detected files to quarantine. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, please refer to "*Managing quarantined files*" (p. 93).

**Deny access**

In case an infected file is detected, the access to this will be denied.

### 18.1.4. Restoring the default settings

The default real-time protection settings ensure good protection against malware, with minor impact on system performance.

To restore the default real-time protection settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Shield** tab.
5. Click **Default**.

## 18.2. On-demand scanning

The main objective for Bitdefender is to keep your computer clean of viruses. This is done by keeping new viruses out of your computer and by scanning your e-mail messages and any new files downloaded or copied to your system.

There is a risk that a virus is already lodged in your system, before you even install Bitdefender. This is why it's a very good idea to scan your computer for resident viruses after you've installed Bitdefender. And it's definitely a good idea to frequently scan your computer for viruses.

On-demand scanning is based on scan tasks. Scan tasks specify the scanning options and the objects to be scanned. You can scan the computer whenever you want by running the default tasks or your own scan tasks (user-defined tasks). If you want to scan specific locations on your computer or to configure the scan options, configure and run a custom scan.

### 18.2.1. Autoscan

Autoscan is a light on-demand scan that silently scans all your data for malware and takes the appropriate actions for any infections found. Autoscan finds and uses time-slices when system resource usage falls below a certain threshold to perform recurring scans of the entire system.

Benefits of using Autoscan:

- It has close to zero impact on the system.
- By pre-scanning the entire hard-disk, future on-demand tasks will be completed extremely fast.
- On-access scanning will also take significantly less time.

To turn on or off Autoscan, follow these steps:

1. Open the Bitdefender window.
2. On the **Antivirus** panel, click the switch to turn on or off **Autoscan**.

### 18.2.2. Scanning a file or folder for malware

You should scan files and folders whenever you suspect they might be infected. Right-click the file or folder you want to be scanned, point to **Bitdefender** and select **Scan with Bitdefender**. The Antivirus Scan wizard will appear and guide you through the scanning process. At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.

### 18.2.3. Running a Quick Scan

Quick Scan uses in-the-cloud scanning to detect malware running in your system. Running a Quick Scan usually takes less than a minute and uses a fraction of the system resources needed by a regular virus scan.

To run a Quick Scan, follow these steps:

1. Open the Bitdefender window.
2. On the **Antivirus** panel, click **Scan Now** and select **Quick Scan** from the drop-down menu.
3. Follow the Antivirus Scan wizard to complete the scan. Bitdefender will automatically take the recommended actions on detected files. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

### 18.2.4. Running a System Scan

The System Scan task scans the entire computer for all types of malware threatening its security, such as viruses, spyware, adware, rootkits and others. If you have turned off Autoscan, it is recommended to run a System Scan at least once a week.

Note

Because **System Scan** performs a thorough scan of the entire system, the scan may take a while. Therefore, it is recommended to run this task when you are not using your computer.

Before running a System Scan, the following are recommended:

- Make sure Bitdefender is up-to-date with its malware signatures. Scanning your computer using an outdated signature database may prevent Bitdefender from detecting new malware found since the last update. For more information, please refer to "*Keeping Bitdefender up-to-date*" (p. 38).
- Shut down all open programs.

If you want to scan specific locations on your computer or to configure the scanning options, configure and run a custom scan. For more information, please refer to "*Configuring a custom scan*" (p. 83).

To run a System Scan, follow these steps:

1. Open the Bitdefender window.
2. On the **Antivirus** panel, click **Scan Now** and select **System Scan** from the drop-down menu.
3. Follow the Antivirus Scan wizard to complete the scan. Bitdefender will automatically take the recommended actions on detected files. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

### 18.2.5. Configuring a custom scan

To configure a scan for malware in detail and then run it, follow these steps:

1. Open the Bitdefender window.
2. On the **Antivirus** panel, click **Scan Now** and select **Manage Scans** from the drop-down menu.
3. Click **New custom task** to enter a name for the scan and select the locations to be scanned.
4. If you want to configure the scanning options in detail, select the **Advanced** tab. A new window will appear. Follow these steps:
   a. You can easily configure the scanning options by adjusting the scan level. Drag the slider along the scale to set the desired scan level. Use the description on the right side of the scale to identify the scan level that better fits your needs.

      Advanced users might want to take advantage of the scan settings Bitdefender offers. To configure the scan options in detail, click **Custom**. You can find information about them at the end of this section.

   b. You can also configure these general options:

      - **Run the task with low priority.** Decreases the priority of the scan process. You will allow other programs to run faster and increase the time needed for the scan process to finish.
      - **Minimize Scan Wizard to system tray.** Minimizes the scan window to the system tray. Double-click the Bitdefender icon to open it.
      - Specify the action to be taken if no threats are found.

   c. Click **OK** to save the changes and close the window.
5. Click **Schedule** if you want to set a schedule for your scan task. Use the switch to turn on or off **Schedule**. Select one of the corresponding options to set a schedule:
   - At system startup
   - Once
   - Periodically
6. Click **Start Scan** and follow the Antivirus Scan wizard to complete the scan. Depending on the locations to be scanned, the scan may take a while. At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.
7. If you want to, you can quickly rerun a previous custom scan by clicking the corresponding entry in the available list.

## Information on the scan options

You may find this information useful:

- If you are not familiar with some of the terms, check them in the glossary. You can also find useful information by searching the Internet.
- **Scan files.** You can set Bitdefender to scan all types of files or applications (program files) only. Scanning all files provides best protection, while scanning applications only can be used to perform a quicker scan.

  Applications (or program files) are far more vulnerable to malware attacks than other types of files. This category includes the following file extensions: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- **Scan options for archives.** Archives containing infected files are not an immediate threat to the security of your system. The malware can affect your system only if the infected file is extracted from the archive and executed without having real-time protection enabled. However, it is recommended to use this option in order to detect and remove any potential threat, even if it is not an immediate threat.

  Note

  Scanning archived files increases the overall scanning time and requires more system resources.

- **Scan boot sectors.** You can set Bitdefender to scan the boot sectors of your hard disk. This sector of the hard disk contains the necessary computer code to start the boot process. When a virus infects the boot sector, the drive may become inaccessible and you may not be able to start your system and access your data.
- **Scan memory.** Select this option to scan programs running in your system's memory.

- **Scan registry.** Select this option to scan registry keys. Windows Registry is a database that stores configuration settings and options for the Windows operating system components, as well as for installed applications.
- **Scan cookies.** Select this option to scan the cookies stored by browsers on your computer.
- **Scan only new and changed files.** By scanning only new and changed files, you may greatly improve overall system responsiveness with a minimum trade-off in security.
- **Ignore commercial keyloggers.** Select this option if you have installed and use commercial keylogger software on your computer. Commercial keyloggers are legitimate computer monitoring software whose most basic function is to record everything that is typed on the keyboard.
- **Scan for rootkits.** Select this option to scan for rootkits and objects hidden using such software.

### 18.2.6. Antivirus Scan Wizard

Whenever you initiate an on-demand scan (for example, right-click a folder, point to Bitdefender and select **Scan with Bitdefender**), the Bitdefender Antivirus Scan wizard will appear. Follow the wizard to complete the scanning process.

Note

If the scan wizard does not appear, the scan may be configured to run silently, in the background. Look for the scan progress icon in the system tray. You can click this icon to open the scan window and to see the scan progress.

#### Step 1 - Perform scan

Bitdefender will start scanning the selected objects. You can see real-time information about the scan status and statistics (including the elapsed time, an estimation of the remaining time and the number of detected threats). To see more details, click the **Show more** link.

Wait for Bitdefender to finish scanning. The scanning process may take a while, depending on the complexity of the scan.

**Stopping or pausing the scan.** You can stop scanning anytime you want by clicking **Stop&Yes**. You will go directly to the last step of the wizard. To temporarily stop the scanning process, just click **Pause**. You will have to click **Resume** to resume scanning.

**Password-protected archives.** When a password-protected archive is detected, depending on the scan settings, you may be prompted to provide the password. Password-protected archives cannot be scanned unless you provide the password. The following options are available:

- **Password.** If you want Bitdefender to scan the archive, select this option and type the password. If you do not know the password, choose one of the other options.
- **Don't ask for a password and skip this object from scan.** Select this option to skip scanning this archive.
- **Skip all password-protected items without scanning them.** Select this option if you do not want to be bothered about password-protected archives. Bitdefender will not be able to scan them, but a record will be kept in the scan log.

Choose the desired option and click **OK** to continue scanning.

### Step 2 - Choose actions

At the end of the scan, you will be prompted to choose the actions to be taken on the detected files, if any.

Note

When you run a quick scan or a full system scan, Bitdefender will automatically take the recommended actions on detected files during the scan. If there remain unresolved threats, you will be prompted to choose the actions to be taken on them.

The infected objects are displayed in groups, based on the malware they are infected with. Click the link corresponding to a threat to find out more information about the infected objects.

You can choose an overall action to be taken for all issues or you can select separate actions for each group of issues. One or several of the following options can appear on the menu:

**Take proper actions**

Bitdefender will take the recommended actions depending on the type of detected file:

- **Infected files.** Files detected as infected match a malware signature in the Bitdefender Malware Signature Database. Bitdefender will automatically attempt to remove the malware code from the infected file and reconstruct the original file. This operation is referred to as disinfection.

  Files that cannot be disinfected are moved to quarantine in order to contain the infection. Quarantined files cannot be executed or opened; therefore, the risk of getting infected disappears. For more information, please refer to "*Managing quarantined files*" (p. 93).

Important

For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

- **Suspicious files.** Files are detected as suspicious by the heuristic analysis. Suspicious files cannot be disinfected, because no disinfection routine is available. They will be moved to quarantine to prevent a potential infection.

  By default, quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

- **Archives containing infected files.**
  - Archives that contain only infected files are deleted automatically.
  - If an archive contains both infected and clean files, Bitdefender will attempt to delete the infected files provided it can reconstruct the archive with the clean files. If archive reconstruction is not possible, you will be informed that no action can be taken so as to avoid losing clean files.

**Delete**

Removes detected files from the disk.

If infected files are stored in an archive together with clean files, Bitdefender will attempt to delete the infected files and reconstruct the archive with the clean files. If archive reconstruction is not possible, you will be informed that no action can be taken so as to avoid losing clean files.

**Take no action**

No action will be taken on the detected files. After the scan is completed, you can open the scan log to view information on these files.

Click **Continue** to apply the specified actions.

### Step 3 - Summary

When Bitdefender finishes fixing the issues, the scan results will appear in a new window. If you want comprehensive information on the scanning process, click **Show Log** to view the scan log.

Click **Close** to close the window.

Important

In most cases Bitdefender successfully disinfects the infected files it detects or it isolates the infection. However, there are issues that cannot be solved automatically. If required, please restart your system in order to complete the cleaning process. For more information and instructions on how to remove malware manually, please refer to "*Removing malware from your system*" (p. 192).

### 18.2.7. Checking scan logs

Each time a scan is performed, a scan log is created and Bitdefender records the detected issues in the Antivirus Overview window. The scan log contains detailed information about the logged scanning process, such as scanning options, the scanning target, the threats found and the actions taken on these threats.

You can open the scan log directly from the scan wizard, once the scan is completed, by clicking **Show Log**.

To check a scan log or any detected infection at a later time, follow these steps:

1. Open the Bitdefender window.
2. Click the **Events** button on the upper toolbar.
3. In the **Events Overview** window, select **Antivirus**.
4. In the **Antivirus Events** window, select the **Virus Scan** tab. This is where you can find all malware scan events, including threats detected by on-access scanning, user-initiated scans and status changes for automatic scans.
5. In the events list, you can check what scans have been performed recently. Click an event to view details about it.
6. To open the scan log, click **View log**.

## 18.3. Automatic scan of removable media

Bitdefender automatically detects when you connect a removable storage device to your computer and scans it in the background. This is recommended in order to prevent viruses and other malware from infecting your computer.

Detected devices fall into one of these categories:

- CDs/DVDs
- USB storage devices, such as flash pens and external hard-drives
- mapped (remote) network drives

You can configure automatic scan separately for each category of storage devices. Automatic scan of mapped network drives is off by default.

### 18.3.1. How does it work?

When it detects a removable storage device, Bitdefender starts scanning it for malware in the background (provided automatic scan is enabled for that type of device). A Bitdefender scan icon will appear in the system tray. You can click this icon to open the scan window and to see the scan progress.

If Autopilot is on, you will not be bothered about the scan. The scan will only be logged and information about it will be available in the Events window.

If Autopilot is off:

1. You will be notified through a pop-up window that a new device has been detected and it is being scanned.
2. In most cases, Bitdefender automatically removes detected malware or isolates infected files into quarantine. If there are unresolved threats after the scan, you will be prompted to choose the actions to be taken on them.

Note

Take into account that no action can be taken on infected or suspicious files detected on CDs/DVDs. Similarly, no action can be taken on infected or suspicious files detected on mapped network drives if you do not have the appropriate privileges.

3. When the scan is completed, the scan results window is displayed to inform you if you can safely access files on the removable media.

This information may be useful to you:

- Please be careful when using a malware-infected CD/DVD, because the malware cannot be removed from the disc (the media is read-only). Make sure real-time protection is turned on to prevent malware from spreading to your system. It is best practice to copy any valuable data from the disc to your system and then dispose of the disc.
- In some cases, Bitdefender may not be able to remove malware from specific files due to legal or technical constraints. Such an example are files archived using a proprietary technology (this is because the archive cannot be recreated correctly).

  To find out how to deal with malware, please refer to "*Removing malware from your system*" (p. 192).

## 18.3.2. Managing removable media scan

To manage automatic scan of removable media, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Exclusions** tab.

For best protection, it is recommended to turn on automatic scan for all types of removable storage devices.

The scanning options are pre-configured for the best detection results. If infected files are detected, Bitdefender will try to disinfect them (remove the malware code) or to move them to quarantine. If both actions fail, the Antivirus Scan wizard will

allow you to specify other actions to be taken on infected files. The scanning options are standard and you cannot change them.

## 18.4. Configuring scan exclusions

Bitdefender allows excluding specific files, folders or file extensions from scanning. This feature is intended to avoid interference with your work and it can also help improve system performance. Exclusions are to be used by users having advanced computer knowledge or, otherwise, following the recommendations of a Bitdefender representative.

You can configure exclusions to apply to on-access or on-demand scanning only, or to both. The objects excluded from on-access scanning will not be scanned, no matter if they are accessed by you or by an application.

Note

Exclusions will NOT apply for contextual scanning. Contextual scanning is a type of on-demand scanning: you right-click the file or folder you want to scan and select **Scan with Bitdefender**.

### 18.4.1. Excluding files or folders from scanning

To exclude specific files or folders from scanning, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Exclusions** tab.
5. Turn on scan exclusions for files using the corresponding switch.
6. Click the **Excluded files and folders** link. In the window that appears, you can manage the files and folders excluded from scanning.
7. Add exclusions by following these steps:
   a. Click the **Add** button, located at the top of the exclusions table.
   b. Click **Browse**, select the file or folder that you want to be excluded from scanning and then click **OK**. Alternatively, you can type (or copy and paste) the path to the file or folder in the edit field.
   c. By default, the selected file or folder is excluded from both on-access and on-demand scanning. To change when to apply the exclusion, select one of the other options.
   d. Click **Add**.
8. Click **OK** to save the changes and close the window.

### 18.4.2. Excluding file extensions from scanning

When you exclude a file extension from scanning, Bitdefender will no longer scan files with that extension, regardless of their location on your computer. The exclusion also applies to files on removable media, such as CDs, DVDs, USB storage devices or network drives.

Important
Use caution when excluding extensions from scanning because such exclusions can make your computer vulnerable to malware.

To exclude file extensions from scanning, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Exclusions** tab.
5. Turn on scan exclusions for files using the corresponding switch.
6. Click the **Excluded extensions** link. In the window that appears, you can manage the file extensions excluded from scanning.
7. Add exclusions by following these steps:
   a. Click the **Add** button, located at the top of the exclusions table.
   b. Enter the extensions that you want to be excluded from scanning, separating them with semicolons (;). Here is an example:

      ```
      txt;avi;jpg
      ```

   c. By default, all files with the specified extensions are excluded from both on-access and on-demand scanning. To change when to apply the exclusion, select one of the other options.
   d. Click **Add**.
8. Click **OK** to save the changes and close the window.

### 18.4.3. Managing scan exclusions

If the configured scan exclusions are no longer needed, it is recommended that you delete them or disable scan exclusions.

To manage scan exclusions, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.

4. In the **Antivirus Settings** window, select the **Exclusions** tab. Use the options in the **Files and folders** section to manage scan exclusions.
5. To remove or edit scan exclusions, click one of the available links. Proceed as follows:
   - To remove an entry from the table, select it and click the **Remove** button.
   - To edit an entry from the table, double-click it (or select it and click the **Edit** button). A new window will appear where you can change the extension or the path to be excluded and the type of scanning you want them to be excluded from, as needed. Make the necessary changes, then click **Modify**.
6. To turn off scan exclusions, use the corresponding switch.

## 18.5. Managing quarantined files

Bitdefender isolates the malware-infected files it cannot disinfect and the suspicious files in a secure area named quarantine. When a virus is in quarantine it cannot do any harm because it cannot be executed or read.

By default, quarantined files are automatically sent to Bitdefender Labs in order to be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

In addition, Bitdefender scans the quarantined files after each malware signature update. Cleaned files are automatically moved back to their original location.

To check and manage quarantined files, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Quarantine** tab.
5. Quarantined files are managed automatically by Bitdefender according to the default quarantine settings. Though not recommended, you can adjust the quarantine settings according to your preferences.

   **Rescan quarantine after virus definitions update**
   Keep this option turned on to automatically scan quarantined files after each virus definitions update. Cleaned files are automatically moved back to their original location.

   **Submit suspicious quarantined files for further analysis**
   Keep this option turned on to automatically send quarantined files to Bitdefender Labs. The sample files will be analyzed by the Bitdefender malware researchers. If malware presence is confirmed, a signature is released to allow removing the malware.

**Delete content older than {30} days**
By default, quarantined files older than 30 days are automatically deleted. If you want to change this interval, type a new value in the corresponding field. To disable automatic deletion of old quarantined files, type 0.

6. To delete a quarantined file, select it and click the **Delete** button. If you want to restore a quarantined file to its original location, select it and click **Restore**.

## 18.6. Active Virus Control

Bitdefender Active Virus Control is an innovative proactive detection technology which uses advanced heuristic methods to detect new potential threats in real time.

Active Virus Control continuously monitors the applications running on the computer, looking for malware-like actions. Each of these actions is scored and an overall score is computed for each process. When the overall score for a process reaches a given threshold, the process is considered to be harmful and it is blocked automatically.

If Autopilot is off, you will be notified through a pop-up window about the blocked application. Otherwise, the application will be blocked without any notification. You can check what applications have been detected by Active Virus Control in the Events window.

### 18.6.1. Checking detected applications

To check the applications detected by Active Virus Control, follow these steps:

1. Open the Bitdefender window.
2. Click the **Events** button on the upper toolbar.
3. In the **Events Overview** window, select **Antivirus**.
4. In the **Antivirus Events** window, select the **Active Virus Control** tab.
5. Click an event to view details about it.
6. If you trust the application, you can configure Active Virus Control not to block it anymore by clicking **Allow and monitor**. Active Virus Control will continue to monitor excluded applications. If an excluded application is detected to perform suspicious activities, the event will simply be logged and reported to Bitdefender Cloud as detection error.

### 18.6.2. Turning on or off Active Virus Control

To turn on or off Active Virus Control, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.

4. In the **Antivirus Settings** window, select the **Shield** tab.
5. Click the switch to turn on or off Active Virus Control.

### 18.6.3. Adjusting the Active Virus Control protection

If you notice that Active Virus Control detects legitimate applications often, you should set a more permissive protection level.

To adjust the Active Virus Control protection, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Shield** tab.
5. Make sure Active Virus Control is turned on.
6. Drag the slider along the scale to set the desired protection level. Use the description on the right side of the scale to choose the protection level that better fits your security needs.

Note
As you set the protection level higher, Active Virus Control will require fewer signs of malware-like behavior to report a process. This will lead to a higher number of applications being reported and, at the same time, to an increased likelihood of false positives (clean applications detected as malicious).

### 18.6.4. Managing excluded processes

You can configure exclusion rules for trusted applications so that Active Virus Control does not block them if they perform malware-like actions. Active Virus Control will continue to monitor excluded applications. If an excluded application is detected to perform suspicious activities, the event will simply be logged and reported to Bitdefender Cloud as detection error.

To manage Active Virus Control process exclusions, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Exclusions** tab.
5. Click the **Excluded processes** link. In the window that appears, you can manage the Active Virus Control process exclusions.

Note

Process exclusions also apply to the Intrusion Detection System included in the Bitdefender firewall.

6. Add exclusions by following these steps:
   a. Click the **Add** button, located at the top of the exclusions table.
   b. Click **Browse**, find and select the application you want to be excluded and then click **OK**.
   c. Keep the **Allow** option selected to prevent Active Virus Control from blocking the application.
   d. Click **Add**.
7. To remove or edit exclusions, proceed as follows:
   - To remove an entry from the table, select it and click the **Delete** button.
   - To edit an entry from the table, double-click it (or select it) and click the **Modify** button. Make the necessary changes, then click **Modify**.
8. Save the changes and close the window.

## 18.7. Fixing system vulnerabilities

An important step in protecting your computer against malicious persons and applications is to keep up to date the operating system and the applications you regularly use. You should also consider disabling Windows settings that make the system more vulnerable to malware. Moreover, to prevent unauthorized physical access to your computer, strong passwords (passwords that cannot be easily guessed) must be configured for each Windows user account.

Bitdefender provides two easy ways to fix the vulnerabilities of your system:

- You can scan your system for vulnerabilities and fix them step by step using the **Vulnerability Scan** wizard.
- Using automatic vulnerability monitoring, you can check and fix detected vulnerabilities in the Events window.

You should check and fix system vulnerabilities every one or two weeks.

### 18.7.1. Scanning your system for vulnerabilities

To fix system vulnerabilities using the Vulnerability Scan wizard, follow these steps:

1. Open the Bitdefender window.
2. On the **Antivirus** panel, click **Scan Now** and select **Vulnerability Scan** from the drop-down menu.

3. Follow the six-step guided procedure to remove vulnerabilities from your system. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.

   a. **Protect your PC**

      Select vulnerabilities to check.

   b. **Check for issues**

      Wait for Bitdefender to finish checking your system for vulnerabilities.

   c. **Windows updates**

      You can see the list of critical and non-critical Windows updates that are not currently installed on your computer. Select the updates you want to install.

      To initiate the installation of selected updates, click **Next**. Please note that it may take a while to install the updates and some of them may require a system restart to complete the installation. If required, restart the system at your earliest convenience.

   d. **Application updates**

      If an application is not up to date, click the provided link to download the latest version.

   e. **Weak passwords**

      You can see the list of the Windows user accounts configured on your computer and the level of protection their password provides.

      Click **Fix** to modify the weak passwords. You can choose between asking the user to change the password at the next logon or changing the password yourself immediately. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).

   f. **Summary**

      This is where you can view the operation result.

## 18.7.2. Using automatic vulnerability monitoring

Bitdefender scans your system for vulnerabilities regularly, in the background, and keeps records of detected issues in the Events window.

To check and fix the detected issues, follow these steps:

1. Open the Bitdefender window.
2. Click the **Events** button on the upper toolbar.
3. In the **Events Overview** window, select **Antivirus**.
4. In the **Antivirus Events** window, select the **Vulnerability** tab.

5. You can see detailed information regarding the detected system vulnerabilities. Depending on the issue, to fix a specific vulnerability proceed as follows:
   - If Windows updates are available, click **Update now** to open the Vulnerability Scan wizard and install them.
   - If an application is outdated, click **Update now** to find a link to the vendor web page from where you can install the latest version of that application.
   - If a Windows user account has a weak password, click **Fix password** to force the user to change the password at the next logon or change the password yourself. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).
   - If the Windows Autorun feature is enabled, click **Disable** to disable it.

To configure the vulnerability monitoring settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Events** window, select the **Vulnerability** tab.
5. Click the switch to turn on or off Automatic Vulnerability Scan.

Important
To be automatically notified about system or application vulnerabilities, keep the **Automatic Vulnerability Scan** enabled.

6. Choose the system vulnerabilities you want to be regularly checked by using the corresponding switches.

   **Critical Windows updates**
   Check if your Windows operating system has the latest critical security updates from Microsoft.

   **Regular Windows updates**
   Check if your Windows operating system has the latest regular security updates from Microsoft.

   **Application updates**
   Check if crucial web-related applications installed on your system are up-to-date. Outdated applications can be exploited by malicious software, making your PC vulnerable to outside attacks.

   **Weak passwords**
   Check whether the passwords of the Windows accounts configured on the system are easy to guess or not. Setting passwords that are hard to guess (strong passwords) makes it very difficult for hackers to break into your

system. A strong password includes uppercase and lowercase letters, numbers and special characters (such as #, $ or @).

**Media autorun**

Check the status of the Windows Autorun feature. This feature enables applications to be automatically started from CDs, DVDs, USB drives or other external devices.

Some types of malware use Autorun to spread automatically from removable media to the PC. This is why it is recommended to disable this Windows feature.

Note

If you turn off monitoring of a specific vulnerability, related issues will no longer be recorded in the Events window.

# 19. Antispam

Spam is a term used to describe unsolicited e-mail. Spam is a growing problem, both for individuals and for organizations. It's not pretty, you wouldn't want your kids to see it, it can get you fired (for wasting too much time or from receiving porn in your office mail) and you can't stop people from sending it. The next best thing to that is, obviously, to stop receiving it. Unfortunately, Spam comes in a wide range of shapes and sizes, and there's a lot of it.

Bitdefender Antispam employs remarkable technological innovations and industry standard antispam filters to weed out spam before it reaches the user's Inbox. For more information, please refer to "*Antispam insights*" (p. 100).

The Bitdefender Antispam protection is available only for e-mail clients configured to receive e-mail messages via the POP3 protocol. POP3 is one of the most widely used protocols for downloading e-mail messages from a mail server.

Note

Bitdefender does not provide antispam protection for e-mail accounts that you access through a web-based e-mail service.

The spam messages detected by Bitdefender are marked with the `[spam]` prefix in the subject line. Bitdefender automatically moves spam messages to a specific folder, as follows:

- In Microsoft Outlook, spam messages are moved to a **Spam** folder, located in the **Deleted Items** folder. The **Spam** folder is created during the installation of Bitdefender.
- In Outlook Express and Windows Mail, spam messages are moved directly to **Deleted Items**.
- In Mozilla Thunderbird, spam messages are moved to a **Spam** folder, located in the **Trash** folder. The **Spam** folder is created during the installation of Bitdefender.

If you use other mail clients, you must create a rule to move the e-mail messages marked as `[spam]` by Bitdefender to a custom quarantine folder.

## 19.1. Antispam insights

### 19.1.1. Antispam filters

The Bitdefender Antispam Engine incorporates cloud protection and other several different filters that ensure your Inbox to be SPAM-free, like Friends list, Spammers list and Charset filter.

### Friends list / Spammers list

Most people communicate regularly to a group of people or even receive messages from companies or organizations in the same domain. By using **friends or spammers list**, you can easily classify which people you want to receive e-mail from (friends) no matter what the message contains, or which people you never want to hear from again (spammers).

Note

We recommend that you add your friends' names and e-mail addresses to the **Friends list**. Bitdefender does not block messages from those on the list; therefore, adding friends helps ensure that legitimate messages get through.

### Charset filter

Many spam messages are written in Cyrillic and / or Asian charsets. The Charset Filter detects this kind of messages and tags them as SPAM.

## 19.1.2. Antispam operation

The Bitdefender Antispam Engine uses all antispam filters combined to determine whether a certain e-mail message should get into your **Inbox** or not.

Every e-mail that comes from the Internet is first checked with the Friends list/Spammers list filter. If the sender's address is found in the Friends list the e-mail is moved directly to your **Inbox**.

Otherwise, the Spammers list filter will take over the e-mail to verify if the sender's address is on its list. If a match is made, the e-mail will be tagged as SPAM and moved in the **Spam** folder.

Else, the Charset filter will check if the e-mail is written in Cyrillic or Asian characters. If so the e-mail will be tagged as SPAM and moved in the **Spam** folder.

Note

If the e-mail is tagged as SEXUALLY EXPLICIT in the subject line, Bitdefender will consider it SPAM.

## 19.1.3. Supported e-mail clients and protocols

Antispam protection is provided for all POP3/SMTP e-mail clients. The Bitdefender Antispam toolbar however is integrated only into:

- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express and Windows Mail (on 32-bit systems)
- Mozilla Thunderbird 3.0.4

## 19.2. Turning on or off antispam protection

Antispam protection is enabled by default.

To turn off the Antispam module, follow these steps:

1. Open the Bitdefender window.
2. On the **Antispam** panel, click the switch to turn on or off **Antispam**.

## 19.3. Using the antispam toolbar in your mail client window

In the upper area of your mail client window you can see the Antispam toolbar. The Antispam toolbar helps you manage antispam protection directly from your mail client. You can easily correct Bitdefender if it marked a legitimate message as SPAM.

Important

Bitdefender integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, please refer to "*Supported e-mail clients and protocols*" (p. 101).

Each button from the Bitdefender toolbar will be explained below:

**Is Spam** - indicates that the selected e-mail is spam. The e-mail will be moved immediately to the **Spam** folder. If the antispam cloud services are activated, the message is sent to Bitdefender Cloud for further analysis.

**Not Spam** - indicates that the selected e-mail is not spam and Bitdefender should not have tagged it. The e-mail will be moved from the **Spam** folder to the **Inbox** directory. If the antispam cloud services are activated, the message is sent to Bitdefender Cloud for further analysis.

Important

The **Not Spam** button becomes active when you select a message marked as SPAM by Bitdefender (normally these messages are located in the **Spam** folder).

**Add Spammer** - adds the sender of the selected e-mail to the Spammers list. You may need to click **OK** to acknowledge. The e-mail messages received from addresses in the Spammers list are automatically marked as `[spam]`.

**Add Friend** - adds the sender of the selected e-mail to the Friends list. You may need to click **OK** to acknowledge. You will always receive e-mail messages from this address no matter what they contain.

**Spammers** - opens the **Spammers list** that contains all the e-mail addresses from which you don't want to receive messages, regardless of their content. For more information, please refer to "*Configuring the Spammers List*" (p. 105).

**Friends** - opens the **Friends list** that contains all the e-mail addresses from which you always want to receive e-mail messages, regardless of their content. For more information, please refer to "*Configuring the Friends List*" (p. 104).

**Settings** - opens a window where you can configure the antispam filters and the toolbar settings.

### 19.3.1. Indicating detection errors

If you are using a supported mail client, you can easily correct the antispam filter (by indicating which e-mail messages should not have been marked as [spam]). Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the junk mail folder where spam messages are moved.
3. Select the legitimate message incorrectly marked as [spam] by Bitdefender.
4. Click the **Add Friend** button on the Bitdefender antispam toolbar to add the sender to the Friends list. You may need to click **OK** to acknowledge. You will always receive e-mail messages from this address no matter what they contain.
5. Click the **Not Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). The e-mail message will be moved to the Inbox folder.

### 19.3.2. Indicating undetected spam messages

If you are using a supported mail client, you can easily indicate which e-mail messages should have been detected as spam. Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the Inbox folder.
3. Select the undetected spam messages.
4. Click the **Is Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). They are immediately marked as [spam] and moved to the junk mail folder.

### 19.3.3. Configuring toolbar settings

To configure the antispam toolbar settings for your e-mail client, click **Settings** button on the toolbar and then the **Toolbar Settings** tab.

Here you have the following options:

- **Move message to Deleted Items** (only for Microsoft Outlook Express / Windows Mail)

Note

In Microsoft Outlook / Mozilla Thunderbird, detected spam messages are automatically moved to a Spam folder, located in the Deleted Items / Trash folder.

- **Mark spam e-mail messages as 'read'** - marks the spam messages as read automatically, so as not to be disturbing when they arrive.
- You can choose whether or not to display confirmation windows when you click the **Add Spammer** and **Add Friend** buttons on the antispam toolbar.

  Confirmation windows can prevent accidentally adding e-mail senders to Friends / Spammers list.

## 19.4. Configuring the Friends List

The **Friends list** is a list of all the e-mail addresses from which you always want to receive messages, regardless of their content. Messages from your friends are not labeled as spam, even if the content resembles spam.

Note

Any mail coming from an address contained in the **Friends list**, will automatically be delivered to your Inbox without further processing.

To configure and manage the Friends list:

- If you are using Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, click the **Friends** button on the Bitdefender antispam toolbar.
- Alternatively, follow these steps:
  1. Open the Bitdefender window.
  2. On the **Antispam** panel, click **Manage** and select **Manage Friends** from the drop-down menu.

To add an e-mail address, select the **E-mail address** option, enter the address and then click **Add**. Syntax: name@domain.com.

To add all the e-mail addresses from a specific domain, select the **Domain name** option, enter the domain name and then click **Add**. Syntax:

- @domain.com, *domain.com and domain.com - all the received e-mail messages from domain.com will reach your **Inbox** regardless of their content;
- *domain* - all the received e-mail messages from domain (no matter the domain suffixes) will reach your **Inbox** regardless of their content;
- *com - all the received e-mail messages having the domain suffix com will reach your **Inbox** regardless of their content;

It is recommended to avoid adding entire domains, but this may be useful in some situations. For example, you can add the e-mail domain of the company you work for, or those of your trusted partners.

To delete an item from the list, click the corresponding **Remove** link. To delete all entries from the list, click the **Clear list** button and then **Yes** to confirm.

You can save the Friends list to a file so that you can use it on another computer or after reinstalling the product. To save the Friends list, click the **Save** button and save it to the desired location. The file will have a `.bwl` extension.

To load a previously saved Friends list, click the **Load** button and open the corresponding `.bwl` file. To reset the content of the existing list when loading a previously saved list, select **Overwrite the current list**.

Click **OK** to save the changes and close the window.

## 19.5. Configuring the Spammers List

The **Spammers list** is a list of all the e-mail addresses from which you don't want to receive messages, regardless of their content. Any e-mail message received from an address contained in the **Spammers list** will be automatically marked as SPAM, without further processing.

To configure and manage the Spammers list:

- If you are using Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, click **Spammers** button on the Bitdefender antispam toolbar integrated into your mail client.
- Alternatively, follow these steps:
  1. Open the Bitdefender window.
  2. On the **Antispam** panel, click **Manage** and select **Manage Spammers** from the drop-down menu.

To add an e-mail address, select the **E-mail address** option, enter the address and then click **Add**. Syntax: name@domain.com.

To add all the e-mail addresses from a specific domain, select the **Domain name** option, enter the domain name and then click **Add**. Syntax:

- @domain.com, *domain.com and domain.com - all the received e-mail messages from domain.com will be tagged as SPAM;
- *domain* - all the received e-mail messages from domain (no matter the domain suffixes) will be tagged as SPAM;
- *com - all the received e-mail messages having the domain suffix com will be tagged as SPAM.

It is recommended to avoid adding entire domains, but this may be useful in some situations.

Warning

Do not add domains of legitimate web-based e-mail services (such as Yahoo, Gmail, Hotmail or other) to the Spammers list. Otherwise, the e-mail messages received from any registered user of such a service will be detected as spam. If, for example, you add `yahoo.com` to the Spammers list, all e-mail messages coming from `yahoo.com` addresses will be marked as `[spam]`.

To delete an item from the list, click the corresponding **Remove** link. To delete all entries from the list, click the **Clear list** button and then **Yes** to confirm.

You can save the Spammers list to a file so that you can use it on another computer or after reinstalling the product. To save the Spammers list, click the **Save** button and save it to the desired location. The file will have a `.bwl` extension.

To load a previously saved Spammers list, click the **Load** button and open the corresponding `.bwl` file. To reset the content of the existing list when loading a previously saved list, select **Overwrite the current list**.

Click **OK** to save the changes and close the window.

## 19.6. Configuring the local antispam filters

As described in "*Antispam insights*" (p. 100), Bitdefender uses a combination of different antispam filters to identify spam. The antispam filters are pre-configured for efficient protection.

Important

Depending on whether or not you receive legitimate e-mails written in Asian or Cyrillic characters, disable or enable the setting that automatically blocks such e-mails. The corresponding setting is disabled in the localized versions of the program that use such charsets (for example, in the Russian or Chinese version).

To configure the local antispam filters, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antispam**.
4. In the **Antispam Settings** window you have the **Settings** tab.
5. Click the switches to turn on or off the local antispam filters.

If you are using Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, you can configure the local antispam filters directly from your mail client. Click the **Settings** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window) and then the **Antispam Filters** tab.

## 19.7. Configuring the cloud settings

The cloud detection makes use of the Bitdefender Cloud services to provide you with efficient and always up-to-date antispam protection.

The cloud protection functions as long as you keep Bitdefender Antispam enabled.

Samples of legitimate or spam e-mails can be submitted to Bitdefender Cloud when you indicate detection errors or undetected spam e-mails. This helps improve the Bitdefender antispam detection.

Configure the e-mail sample submission to Bitdefender Cloud by selecting the desired options, by following these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antispam**.
4. Select the desired options from the **Settings** tab.

If you are using Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, you can configure the cloud detection directly from your mail client. Click the **Settings** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window) and then the **Cloud Settings** tab.

# 20. Privacy Control

Your private information is a constant target for cyber criminals. As the threats have spread to nearly the entire spectrum of online activities, improperly protected e-mail, instant messaging and web browsing can lead to information leaks that compromise your privacy.

Additionally, important files you store on your computer can one day find themselves in the wrong hands.

Bitdefender Privacy Control addresses all these threats with a multitude of components.

- Antiphishing Protection - offers a comprehensive set of features that protect your entire web browsing experience, including preventing you from disclosing personal information to fraudulent websites disguised as legitimate ones.
- Chat Encryption - encrypts your IM conversations to ensure their contents remain between you and your chat partner.
- Data Protection - helps you make sure that your personal information is not sent from your computer without your consent. It scans the e-mail and instant messages sent from your computer, as well as any data sent via web pages, and blocks any piece of information protected by the Data Protection rules you have created.
- File Encryption - enables you to create encrypted, password-protected logical drives (or vaults) on your computer where you can securely store your confidential and sensitive documents.
- File Shredder - permanently erases files and their traces from your computer.

## 20.1. Antiphishing protection

Bitdefender Antiphishing prevents you from disclosing personal information while browsing the Internet by alerting you about potential phishing web pages.

Bitdefender provides real-time antiphishing protection for:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera
- Yahoo! Messenger

To configure Antiphishing settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Privacy Control**.

4. In the **Privacy Control Settings** window, select the **Antiphishing** tab.

Click the switches to turn on or off:

- Showing the Bitdefender toolbar in the web browser.

  Note
  The Bitdefender browser toolbar is not enabled by default.

- Search Advisor, a component that rates the results of your search engine queries and the links posted on social networking websites by placing an icon next to every result:

  You should not visit this web page.

  This web page may contain dangerous content. Exercise caution if you decide to visit it.

  This is a safe page to visit.

  Search Advisor rates the search results from the following web search engines:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Search Advisor rates the links posted on the following online social networking services:
  - Facebook
  - Twitter

- Scanning SSL web traffic.

  More sophisticated attacks might use secure web traffic to mislead their victims. It is therefore recommended to enable SSL scanning.

- Protection against fraud.

- Protection against phishing.

- Protection for instant messaging.

You can create a list of web sites that will not be scanned by the Bitdefender Antiphishing engines. The list should contain only web sites you fully trust. For example, add the web sites where you currently shop online.

To configure and manage the antiphishing whitelist, click the **Whitelist** link. A new window will appear.

To add a site to the whitelist, provide its address in the corresponding field and click **Add**.

To remove a web site from the list, select it in the list and click the corresponding **Remove** link.

Click **Save** to save the changes and close the window.

### 20.1.1. Bitdefender protection in the web browser

Bitdefender integrates directly through an intuitive and easy-to-use toolbar into the following web browsers:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari
- Opera

The Bitdefender toolbar is not your typical browser toolbar. The only thing it ads to your browser is a small dragger at the top of every web page. Click it to see the toolbar.

The Bitdefender toolbar contains the following elements:

**Page Rating**

Depending on how Bitdefender classifies the web page you are currently viewing, one of the following ratings is displayed on the left side of the toolbar:

- The message "Page not safe" appears on a red background - you should leave the web page immediately. To find out more about this threat, click the **+** symbol on the page rating.
- The message "Caution is advised" appears on an orange background - this web page may contain dangerous content. Exercise caution if you decide to visit it.
- The message "This page is safe" appears on a green background - this is a safe page to visit.

**Sandbox**

Click to launch the browser in a Bitdefender-provided environment, isolating it from the operating system. This prevents browser-based threats from exploiting browser vulnerabilities to gain control of your system. Use Sandbox when visiting web pages you suspect may contain malware.

Browser windows opened in Sandbox will be easily recognizable through their modified outline and Sandbox icon added at the center of the title bar.

Note
Sandbox is not available on computers running Windows XP.

**Settings**

Click to select individual features to turn on or off:

- Antiphishing Filter
- Antimalware Web Filter
- Search Advisor

**Power Switch**

To enable / disable the toolbar features completely, click on the right side of the toolbar.

### 20.1.2. Bitdefender alerts in the browser

Whenever you try to visit a website classified as unsafe, the website is blocked and a warning page is displayed in your browser.

The page contains information such as the website URL and the detected threat.

You have to decide what to do next. The following options are available:

- Navigate away from the web page by clicking **Take me back to safety**.
- Disable blocking pages that contain phishing by clicking **Disable Antiphishing filter**.
- Disable blocking pages that contain malware by clicking **Disable Antimalware filter**.
- Add the page to the Antiphishing whitelist by clicking **Add to whitelist**.The page will no longer be scanned by Bitdefender Antiphishing engines.
- Proceed to the web page, despite the warning, by clicking **I understand the risks, take me there anyway**.

## 20.2. Chat encryption

The contents of your instant messages should remain between you and your chat partner. By encrypting your conversations, you can make sure anyone trying to intercept them on their way to and from your contacts will not be able to read their contents.

By default, Bitdefender encrypts all your instant messaging chat sessions provided that:

- Your chat partner has a Bitdefender product installed that supports Chat Encryption and Chat Encryption is enabled for the instant messaging application used for chatting.
- You and your chat partner use Yahoo! Messenger.

Important

Bitdefender will not encrypt a conversation if one of the chat partners uses a web-based chat application such as Meebo.

Once the prerequisites are met, Bitdefender will inform you of the encryption status of your chat session through messages displayed in the chat window.

To turn instant messaging encryption on or off follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Privacy Control**.
4. In the **Privacy Control Settings** window, select the **Chat Encryption** tab.
5. Click the switch to turn on or off instant messaging encryption. By default, encryption is enabled.

## 20.3. Data protection

Data protection prevents sensitive data leaks when you are online.

Consider a simple example: you have created a data protection rule that protects your credit card number. If a spyware software somehow manages to install on your computer, it cannot send your credit card number via e-mail, instant messages or web pages. Moreover, your children cannot use it to buy online or reveal it to people they met on the Internet.

### 20.3.1. About data protection

Whether it is your e-mail or your credit card number, when they fall into the wrong hands such information may cause you damage: you may find yourself drowning in spam messages or you might be surprised to access an emptied account.

Based on the rules you create, Data Protection scans the web, e-mail and instant messaging traffic leaving your computer for specific character strings (for example, your credit card number). If there is a match, the respective web page, e-mail or instant message is blocked.

You can create rules to protect any piece of information you might consider personal or confidential, from your phone number or e-mail address to your bank account information. Multiuser support is provided so that users logging on to different Windows user accounts can configure and use their own rules. If your Windows account is an administrator account, the rules you create can be configured to also apply when other users of the computer are logged on to their Windows user accounts.

### 20.3.2. Configuring data protection

If you want to use data protection, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.

3. In the **Settings Overview** window, select **Privacy Control**.
4. In the **Privacy Control Settings** window, select the **Data Protection** tab.
5. Make sure data protection is enabled.
6. Create rules to protect your sensitive data. For more information, please refer to "*Creating data protection rules*" (p. 113).

## Creating data protection rules

To create a rule, click the **Add rule** button and follow the configuration wizard. You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Describe Rule**

   You must set the following parameters:

   - **Rule Name** - type the name of the rule in this edit field.
   - **Rule Type** - choose the rule type (address, name, credit card, PIN, SSN, etc).
   - **Rule Data** - type the data you want to protect in this edit field. For example, if you want to protect your credit card number, type all or part of it here.

     Important
     It is recommended to enter at least three characters in order to avoid mistakenly blocking messages and web pages. However, for extra safety, only enter partial data (for example, only a part of your credit card number).

   - **Rule Description** - enter a short description of the rule in the edit field. Since the blocked data (character string) is not displayed in plain text when accessing the rule, the description should help you easily identify it.

2. **Configure rule settings**

   a. Select the type of traffic you want Bitdefender to scan.

      - **Scan Web (HTTP traffic)** - scans the HTTP (web) traffic and blocks the outgoing data that matches the rule data.
      - **Scan e-mail (SMTP traffic)** - scans the SMTP (mail) traffic and blocks the outgoing e-mail messages that contain the rule data.

      You can choose to apply the rule only if the rule data matches whole words or if the rule data and the detected string case match.

   b. Specify the users for which the rule applies.

      - **Only for me (current user)** - the rule will apply only to your user account.
      - **All users** - the rule will apply to all Windows accounts.

- **Limited user accounts** - the rule will apply to you and all limited Windows accounts.

Click **Finish**. The rule will appear in the table.

From now on, any attempt to send the rule data through the selected protocols will fail. An entry will be displayed in the Events window indicating that Bitdefender has blocked identity specific content from being sent.

### 20.3.3. Managing rules

To manage the data protection rules:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Privacy Control**.
4. In the **Privacy Control Settings** window, select the **Data Protection** tab.

You can see the rules created so far listed in the table.

To delete a rule, select it and click the **Remove rule** button.

To edit a rule, select it and click the **Edit rule** button. A new window will appear. Here you can change the name, description and parameters of the rule (type, data and traffic). Click **OK** to save the changes.

## 20.4. File encryption

Bitdefender File Encryption enables you to create encrypted, password-protected logical drives (or vaults) on your computer where you can securely store your confidential and sensitive documents. The data stored on the vaults can only be accessed by users who know the password.

The password allows you to open, store data on and close a vault while maintaining its security. While a vault is open, you can add new files, access current files or change them.

Physically, the vault is a file stored on the local hard drive having the `.bvd` extension. Although the physical files representing the vaulted drives can be accessed from a different operating system (such as Linux), the information stored on them cannot be read because it is encrypted.

File vaults can be managed from the Bitdefender window or by using the Windows contextual menu and logical drive associated with the vault.

### 20.4.1. Managing file vaults from the Bitdefender interface

To manage your file vaults from the Bitdefender interface, follow these steps:

1. Open the Bitdefender window.

2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **File Encryption**.
4. In the **File Encryption** window, select the **Encryption** tab.

The existing file vaults appear in the table on the lower part of the window. To refresh the list, right-click inside the table and select **Refresh vaults** in the menu that appears.

## Creating file vaults

To create a new vault, right-click the vaults table header and select **Create File Vault**.

A new window will appear.

1. Specify the location and the name of the vault file.
   - Click **Browse**, select the location of the vault and save the vault file under the desired name.
   - Type the name and the path of the vault file on the disk in the corresponding fields.
2. Choose a drive letter from the menu. When you open the vault, a virtual disk drive labeled with the selected letter appears in My Computer.
3. If you want to change the default size (50 MB) of the vault, type the desired value in the **Vault size** field.
4. Type the desired password to the vault in the **Password** and **Confirm** fields. Anyone trying to open the vault and access its files must provide the password.
5. Click **Create** if you only want to create the vault at the selected location. To create and display the vault as a virtual disk drive in My Computer, click **Create&Open**.

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

Note
It may be convenient to save all file vaults to the same location. In this way, you can find them quicker.

## Opening file vaults

In order to access and work with the files stored in a vault, you must open the vault. When you open the vault, a virtual disk drive appears in My Computer. The drive is labeled with the drive letter assigned to the vault.

To open a vault, follow these steps:

1. Click the vault in the table and select **Open vault** in the menu that appears.

   Note
   If a previously created vault does not appear in the table, right-click the vaults table header, select **Add existing vault** and browse to its location.

2. A new window will appear.

   The vault name and path on the disk are displayed. Choose a drive letter from the menu.

3. Type the vault password in the **Password** field.

4. Click **Open**.

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error.

## Adding files to vaults

To start a wizard that will allow you to add files to a vault, follow these steps:

1. Open the Bitdefender window.
2. On the **File Encryption** panel, click **Encrypt** and select **Add Files to Vault** from the drop-down menu.

You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Select files & folders**

   Click **Add target** to select the files/folders that will be added to the vault.

2. **Select File Vault**

   You can select an existing vault, browse for a previously created vault or create a new one in which to add the files.

3. **Create File Vault**

   If you have chosen to create a new vault, this is where you specify the necessary information about it. For more information, please refer to *"Creating file vaults" (p. 115)*

4. **Enter password**

   If you have selected a locked vault, you must enter the password to open it.

5. **Confirm**

   This is where you can review chosen operations.

Note

If you have chosen to create a new file vault, Bitdefender will prompt you to format the drive associated with it. Select the formatting options and click **Start** to format the drive.

6. **File Vault Content**

   This is where you can view the vault content.

## Locking vaults

When you are done with your work in a file vault, you must lock it in order to protect your data. By locking the vault, the corresponding virtual disk drive disappears from My Computer. Consequently, access to the data stored in the vault is completely blocked.

To lock a vault, click it in the table and select **Lock vault** in the menu that appears.

To start a wizard that will allow you to lock a file vault, follow these steps:

1. Open the Bitdefender window.
2. On the **File Encryption** panel, click **Encrypt** and select **Lock vault** from the drop-down menu.

You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Select File Vault**

   Here you can specify the vault to lock.

2. **Confirm**

   This is where you can review chosen operations.

3. **Finish**

   This is where you can view operation result.

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

## Removing files from vaults

To start a wizard that will allow you to remove files from a vault, follow these steps:

1. Open the Bitdefender window.
2. On the **File Encryption** panel, click **Encrypt** and select **Remove files from vault** from the drop-down menu.

You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Select File Vault**

   Here you can specify the vault to remove files from.

2. **Enter password**

   If you have selected a locked vault, you must enter the password to open it.

3. **File Vault Content**

   Select the files/folders that will be removed from the vault.

4. **Confirm**

   This is where you can review chosen operations.

5. **Finish**

   This is where you can view the operation result.

## Viewing the contents of vaults

To start a wizard that will allow you to view the contents of a file vault, follow these steps:

1. Open the Bitdefender window.
2. On the **File Encryption** panel, click **Encrypt** and select **View vault files** from the drop-down menu.

You can navigate through the wizard using the **Next** and **Back** buttons. To exit the wizard, click **Cancel**.

1. **Select File Vault**

   Here you can specify the vault to view files from.

2. **Enter password**

   If you have selected a locked vault, you must enter the password to open it.

3. **Confirm**

   This is where you can review chosen operations.

4. **File Vault Content**

   This is where you can view the operation result.

## Changing vault password

The vault must be locked before you can change its password. To change the password of a vault, follow these steps:

1. Click the vault in the table and select **Change password** in the menu that appears.

   A new window will appear.

2. Type the current password of the vault in the **Old Password** field.

3. Type the new password of the vault in the **New Password** and **Confirm New Password** fields.

   Note

   The password must have at least 8 characters. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).

4. Click **OK** to change the password.

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

### 20.4.2. Managing file vaults from Windows

Bitdefender integrates into Windows to help you manage your file vaults more easily.

The Windows contextual menu appears whenever you right-click a file or folder on your computer or objects on your desktop. Simply point to Bitdefender File Vault in this menu and you gain access to all available vault operations.

Additionally, whenever you open (mount) a vault a new logical partition (a new drive) will appear. Just open My Computer and you will see a new drive based on your file vault. You will be able to do file operations on it (copy, delete, change, etc). The files are protected as long as they reside on this drive (because a password is required for the mounting operation). When finished, lock (unmount) your vault in order to start protecting its content.

You can easily identify the Bitdefender file vaults on your computer by the Bitdefender icon and the `.bvd` extension.

#### Creating vaults

Keep in mind that a vault is actually just a file with the `.bvd` extension. Only when you open the vault, a virtual disk drive appears in My Computer and you can safely store files inside it. When creating a vault, you must specify where and under which name to save it on your computer. You must also specify a password to protect its content. Only users who know the password can open the vault and access the documents and data stored inside it.

To create a vault, follow these steps:

1. Right-click on your desktop or in a folder on your computer, point to **Bitdefender > Bitdefender File Vault** and select **Create File Vault**. A new window will appear.
2. Specify the location and the name of the vault file.
   - Click **Browse**, select the location of the vault and save the vault file under the desired name.
   - Type the name and the path of the vault file on the disk in the corresponding fields.
3. Choose a drive letter from the menu. When you open the vault, a virtual disk drive labeled with the selected letter appears in My Computer.
4. If you want to change the default size (50 MB) of the vault, type the desired value in the **Vault size** field.
5. Type the desired password to the vault in the **Password** and **Confirm** fields. Anyone trying to open the vault and access its files must provide the password.
6. Click **Create** if you only want to create the vault at the selected location. To create and display the vault as a virtual disk drive in My Computer, click **Create&Open**.

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

Note
It may be convenient to save all file vaults to the same location. In this way, you can find them quicker.

## Opening vaults

In order to access and work with the files stored in a vault, you must open the vault. When you open the vault, a virtual disk drive appears in My Computer. The drive is labeled with the drive letter assigned to the vault.

To open a vault, follow these steps:

1. Locate on your computer the `.bvd` file representing the vault you want to open.
2. Right-click the file, point to **Bitdefender File Vault** and select **Open**. Quicker alternatives would be to double-click the file, or to right-click it and select **Open**. A new window will appear.
3. Choose a drive letter from the menu.
4. Type the vault password in the **Password** field.
5. Click **Open**.

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

## Adding files to vaults

Before you can add files or folders to a vault, you must open the vault. Once a vault is open, you can easily store files or folders inside it using the contextual menu. Right-click the file or folder you want to copy to a vault, point to **Bitdefender File Vault** and click **Add to File Vault**.

- If only one vault is open, the file or folder is copied directly to that vault.
- If several vaults are open, you will be prompted to choose the vault to copy the item to. Select from the menu the drive letter corresponding to the desired vault and click **OK** to copy the item.

You can also use the virtual disk drive corresponding to the vault. Follow these steps:

1. Open My Computer: from the Windows Start screen locate **Computer** (for example, you can start typing "Computer" directly in the Start screen) and then click its icon (on Windows 8); in the Windows Start menu, click **Computer** (on Windows Vista and 7) or **My Computer** (on Windows XP).
2. Enter the virtual disk drive corresponding to the vault. Look for the drive letter you assigned to the vault when you opened it.
3. Copy-paste or drag&drop files and folders directly to this virtual disk drive.

## Locking vaults

When you are done with your work in a file vault, you must lock it in order to protect your data. By locking the vault, the corresponding virtual disk drive disappears from My Computer. Consequently, access to the data stored in the vault is completely blocked.

To lock a vault, follow these steps:

1. Open My Computer: from the Windows Start screen locate **Computer** (for example, you can start typing "Computer" directly in the Start screen) and then click its icon (on Windows 8); in the Windows Start menu, click **Computer** (on Windows Vista and 7) or **My Computer** (on Windows XP).
2. Identify the virtual disk drive corresponding to the vault you want to close. Look for the drive letter you assigned to the vault when you opened it.
3. Right-click the respective virtual disk drive, point to **Bitdefender File Vault** and click **Lock**.

You can also right-click the `.bvd` file representing the vault, point to **Bitdefender File Vault** and click **Lock**.

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

## Removing files from vaults

In order to remove files or folders from a vault, the vault must be open. To remove files or folders from a vault, follow these steps:

1. Open My Computer: from the Windows Start screen locate **Computer** (for example, you can start typing "Computer" directly in the Start screen) and then click its icon (on Windows 8); in the Windows Start menu, click **Computer** (on Windows Vista and 7) or **My Computer** (on Windows XP).
2. Enter the virtual disk drive corresponding to the vault. Look for the drive letter you assigned to the vault when you opened it.
3. Remove files or folders as you normally do in Windows (for example, right-click a file you want to delete and select **Delete**).

## Changing vault password

The password protects the content of a vault from unauthorized access. Only users who know the password can open the vault and access the documents and data stored inside it.

The vault must be locked before you can change its password. To change the password of a vault, follow these steps:

1. Locate on your computer the `.bvd` file representing the vault.
2. Right-click the file, point to **Bitdefender File Vault** and select **Change Vault Password**. A new window will appear.
3. Type the current password of the vault in the **Old Password** field.
4. Type the new password of the vault in the **New Password** and **Confirm New Password** fields.

   Note

   The password must have at least 8 characters. For a strong password, use a combination of uppercase and lowercase letters, numbers and special characters (such as #, $ or @).

5. Click **OK** to change the password.

Bitdefender will immediately inform you about the result of the operation. If an error has occurred, use the error message to troubleshoot the error. Click **OK** to close the window.

## 20.5. Deleting files permanently

When you delete a file, it can no longer be accessed through normal means. However, the file continues to be stored on the hard disk until it is overwritten when copying new files.

The Bitdefender File Shredder will help you permanently delete data by physically removing it from your hard disk.

You can quickly shred files or folders from your computer using the Windows contextual menu, by following these steps:

1. Right-click the file or folder you want to permanently delete.
2. Select **Bitdefender** > **File Shredder** in the context menu that appears.
3. A confirmation window will appear. Click **Yes** to start the File Shredder wizard.
4. Wait for Bitdefender to finish shredding the files.
5. The results are displayed. Click **Close** to exit the wizard.

Alternatively, you can shred files from the Bitdefender interface.

1. Open the Bitdefender window.
2. On the **Privacy** panel, click **Secure** and select **File Shredder** from the drop-down menu.
3. Follow the File Shredder wizard:
   a. **Select file/folder**

      Add the files or folders you want to be permanently removed.

   b. **Shredding Files**

      Wait for Bitdefender to finish shredding the files.

   c. **Results**

      The results are displayed. Click **Close** to exit the wizard.

# 21. Firewall

The Firewall protects your computer from inbound and outbound unauthorized connection attempts, both on local networks and on the Internet. It is quite similar to a guard at your gate - it keeps track of connection attempts and decides which to allow and which to block.

The Bitdefender firewall uses a set of rules to filter data transmitted to and from your system. The rules are grouped into 3 categories:

General Rules

Rules that determine the protocols over which communication is allowed.

A default set of rules that provides an optimal protection is used. You can edit the rules by allowing or denying connections over certain protocols.

Application Rules

Rules that determine how each application can access network resources and the Internet.

Under normal conditions, Bitdefender automatically creates a rule whenever an application tries to access the Internet. You can also manually add or edit rules for applications.

Adapter Rules

Rules that determine whether your computer can communicate with other computers connected to the same network.

You must create rules to specifically allow or deny traffic between your computer and other computers.

If your computer is running Windows Vista, Windows 7 or Windows 8, Bitdefender automatically assigns a network type to every network connection it detects. Depending on the network type, the firewall protection is set to the appropriate level for each connection.

To find out more about the firewall settings for each network type and how you can edit the network settings, please refer to "*Managing connection settings*" (p. 125).

Additional protection is provided by the Intrusion Detection System (IDS). IDS monitors the network and system activities for malicious activities or policy violations. It can detect and block attempts to change critical system files, Bitdefender files or registry entries, the installation of malware drivers and attacks performed by code injection (DLL injection).

Bitdefender is configured by default to take recommended actions for your protection automatically, without bothering you. If you want to be informed and decide on the best action when an application requests Internet access or exhibits suspicious behavior, you must turn on Paranoid Mode.

## 21.1. Turning on or off firewall protection

To turn firewall protection on or off, follow these steps:

1. Open the Bitdefender window.
2. On the **Firewall** panel, click the Firewall switch.

Warning

Because it exposes your computer to unauthorized connections, turning off the firewall should only be a temporary measure. Turn the firewall back on as soon as possible.

## 21.2. Managing connection settings

To view and edit the network connection settings, follow these steps:

1. Open the Bitdefender window.
2. On the **Firewall** panel, click **Manage adapters**.

A new window will appear. The graph at the top of the window shows real-time information regarding incoming and outgoing traffic.

Below the graph, the following information is displayed for each network connection.

- **Network Type** - the type of network your computer is connected to. Bitdefender applies a basic set of firewall settings depending on the type of network you are connected to.

  You can change the type by opening the **Network Type** drop-down menu and selecting one of the available types from the list.

| Network Type | Description |
|---|---|
| **Trusted** | Disable the firewall for the respective adapter. |
| **Home/Office** | Allow all traffic between your computer and computers in the local network. |
| **Public** | All traffic is filtered. |
| **Untrusted** | Completely block network and Internet traffic through the respective adapter. |

- **Stealth Mode** - whether you can be detected by other computers.

  To configure the Stealth Mode, select the desired option from the corresponding drop-down menu.

| Stealth option | Description |
|---|---|
| **On** | Stealth Mode is on. Your computer is invisible from both the local network and the Internet. |
| **Off** | Stealth Mode is off. Anyone from the local network or the Internet can ping and detect your computer. |
| **Remote** | Your computer cannot be detected from the Internet. Local network users can ping and detect your computer. |

- **Generic** - whether generic rules are applied to this connection.

  If the IP address of a network adapter is changed, Bitdefender modifies the network type accordingly. If you want to keep the same type, select **Yes** from the corresponding drop-down menu.

## 21.3. Managing firewall rules

### 21.3.1. General rules

Whenever data is transmitted over the Internet, certain protocols are used.

The general rules allow you to configure the protocols over which traffic is allowed. To edit the rules, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Firewall**.
4. In the **Firewall Settings** window, select the **Settings** tab.
5. Under Firewall Rules, click **General Rules**.

A new window will appear. The current rules are displayed.

To edit a rule, click its corresponding arrow in the **Action** column and select **Allow** or **Deny**.

**DNS over UDP / TCP**
Allow or deny DNS over UDP and TCP.

By default, this type of connection is allowed.

**Incoming ICMP / ICMPv6**
Allow or deny ICMP / ICMPv6 messages.

ICMP messages are often used by hackers to carry out attacks against computer networks. By default, this type of connection is denied.

**Sending E-mails**
Allow or deny sending e-mails over SMTP.

By default, this type of connection is allowed.

**Web Browsing HTTP**
Allow or deny HTTP web browsing.

By default, this type of connection is allowed.

**Incoming Remote Desktop Connections**
Allow or deny other computers' access over Remote Desktop Connections.

By default, this type of connection is allowed.

**Windows Explorer traffic on HTTP / FTP**
Allow or deny HTTP and FTP traffic from Windows Explorer.

By default, this type of connection is denied.

### 21.3.2. Application rules

To view and manage the firewall rules controlling applications' access to network resources and the Internet, click **Application rules**.

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Firewall**.
4. In the **Firewall Settings** window, select the **Settings** tab.
5. Under Firewall Rules, click **Application Rules**.

You can see the programs (processes) for which firewall rules have been created in the table. To see the rules created for a specific application, click the + box next to the respective application or simply double-click it.

For each rule the following information is displayed:

- **Process/Network Types** - the process and the network adapter types the rule applies to. Rules are automatically created to filter network or Internet access through any adapter. You can manually create rules or edit existing rules to filter an application's network or Internet access through a specific adapter (for example, a wireless network adapter).
- **Protocol** - the IP protocol the rule applies to. You may see one of the following:

| Protocol | Description |
|---|---|
| **Any** | Includes all IP protocols. |
| **TCP** | Transmission Control Protocol - TCP enables two hosts to establish a connection and exchange streams of data. TCP guarantees |

| Protocol | Description |
|---|---|
| | delivery of data and also guarantees that packets will be delivered in the same order in which they were sent. |
| **UDP** | User Datagram Protocol - UDP is an IP-based transport designed for high performance. Games and other video-based applications often use UDP. |
| **A number** | Represents a specific IP protocol (other than TCP and UDP). You can find the complete list of assigned IP protocol numbers at http://www.iana.org/assignments/protocol-numbers. |

- **Action** - whether the application is allowed or denied access to the network or Internet under the specified circumstances.

To manage the rules, use the buttons on the lower part of the window:

- **Add rule** - opens the Add Application Rule window where you can create a new rule.
- **Edit rule** - opens the Edit Application Rule window where you can modify the settings of a selected rule.
- **Remove rule** - deletes the selected rule.

## Adding / editing application rules

To add or edit an application rule, click the corresponding button. A new window will appear. Proceed as follows:

- **Program Path.** Click **Browse** and select the application the rule applies to.
- **Local Address.** Specify the local IP address and port the rule applies to. If you have more than one network adapter, you can clear the **Any** check box and type a specific IP address.
- **Remote Address.** Specify the remote IP address and port the rule applies to. To filter traffic between your computer and a specific computer, clear the **Any** check box and type its IP address.
- **Network Type.** Select the type of network the rule applies to.
- **Events.** Depending on the selected protocol, choose the network events the rule applies to. The following events may be taken into account:

| Event | Description |
|---|---|
| **Connect** | Preliminary exchange of standard messages used by connection-oriented protocols (such as TCP) to establish a connection. With connection-oriented protocols, data traffic |

| Event | Description |
|---|---|
| | between two computers occurs only after a connection is established. |
| **Traffic** | Flow of data between two computers. |
| **Listen** | State in which an application monitors the network awaiting to establish a connection or to receive information from a peer application. |

- **Protocol.** Select from the menu the IP protocol the rule applies to.
  - If you want the rule to apply to all protocols, select **Any**.
  - If you want the rule to apply to TCP, select **TCP**.
  - If you want the rule to apply to UDP, select **UDP**.
  - If you want the rule to apply to a specific protocol, select **Other**. An edit field will appear. Type the number assigned to the protocol you want to filter in the edit field.

Note

IP protocol numbers are assigned by the Internet Assigned Numbers Authority (IANA). You can find the complete list of assigned IP protocol numbers at http://www.iana.org/assignments/protocol-numbers.

- **Direction.** Select from the menu the traffic direction the rule applies to.

| Direction | Description |
|---|---|
| **Outbound** | The rule applies only for the outgoing traffic. |
| **Inbound** | The rule applies only for the incoming traffic. |
| **Both** | The rule applies in both directions. |

- **IP version.** Select from the menu the IP version (IPv4, IPv6 or any) the rule applies to.
- **Permission.** Select one of the available permissions:

| Permission | Description |
|---|---|
| **Allow** | The specified application will be allowed network / Internet access under the specified circumstances. |
| **Deny** | The specified application will be denied network / Internet access under the specified circumstances. |

### 21.3.3. Adapter rules

For each network connection you can configure special trusted or untrusted zones.

A trusted zone is a device that you fully trust, for example a computer or a printer. All traffic between your computer and a trusted device is allowed. To share resources with specific computers in an unsecured wireless network, add them as allowed computers.

An untrusted zone is a device that you do not want to communicate with your computer at all.

To view and manage zones on your network adapters, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Firewall**.
4. In the **Firewall Settings** window, select the **Settings** tab.
5. Under Firewall Rules, click **Adapter Rules**.

A new window will appear displaying the network adapters with active connections and the current zones, if any.

To manage the zones, use the buttons on the lower part of the window:

- **Add Zone** - opens the Add IP Address window where you can create a new zone for a selected adapter.
- **Edit Zone** - opens the Edit Rule window where you can modify the settings of a selected zone.
- **Remove Zone** - deletes the selected zone.

#### Adding / editing zones

To add or edit a zone, click the corresponding button. A new window displaying the IP addresses of the devices connected to the network will appear. Proceed as follows:

1. Select the IP address of the computer you want to add, or type an address or address range in the provided text box.
2. Select the action:
   - **Allow** - to allow all traffic between your computer and the selected computer.
   - **Deny** - to block all traffic between your computer and the selected computer.
3. Click **OK** to save the changes and close the window.

## 21.4. Monitoring network activity

To monitor the current network / Internet activity (over TCP and UDP) sorted by application and to open the Bitdefender Firewall log, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Firewall**.
4. In the **Firewall Settings** window, select the **Settings** tab.
5. Under Networks Activity, click **Network activity**.

A new window will appear. You can see the total traffic sorted by application. For each application, you can see the connections and the open ports, as well as statistics regarding the outgoing & incoming traffic speed and the total amount of data sent / received.

An icon is displayed next to each connection. The meaning of the icons is as follows:

- Indicates an outgoing connection.
- Indicates an incoming connection.
- Indicates an open port on your computer.

The window presents the current network / Internet activity in real-time. As connections or ports are closed, you can see that the corresponding statistics are dimmed and that, eventually, they disappear. The same thing happens to all statistics corresponding to an application which generates traffic or has open ports and which you close.

For a comprehensive list of events regarding the Firewall module usage (enabling/disabling firewall, traffic blocking, modifying settings) or generated by the activities detected by this module (scanning ports, blocking connection attempts or traffic according to the rules) view the Bitdefender Firewall log file by clicking **Show Log**. The location of the log file is `?\Program Files\Common Files\Bitdefender\Bitdefender Firewall\bdfirewall.txt`.

## 21.5. Configuring alert intensity

Bitdefender Total Security was designed to be as unintrusive as possible. Under normal conditions, you do not have to make decisions on whether to allow or deny connections or actions attempted by the applications running on your system. Bitdefender makes all the decisions for you.

If you want to be in complete control of the decision making, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.

3. In the **Settings Overview** window, select **Firewall**.
4. In the **Firewall Settings** window, select the **Settings** tab.
5. Turn on **Paranoid Mode** by clicking the corresponding switch.

Note
When Paranoid Mode is turned on, the Autopilot is automatically switched off.

As long as Paranoid Mode is on, an alert will be displayed prompting you for action every time one of the following situations occurs:

- An application tries to connect to the Internet.
- An application tries to perform an action considered suspicious by the Intrusion Detection System or the Active Virus Control.

The alert contains detailed information regarding the application and the detected behavior. You must select to **Allow** or **Deny** the action using the corresponding button.

## 21.6. Configuring advanced settings

To configure advanced firewall settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Firewall**.
4. In the **Firewall Settings** window, select the **Advanced** tab.

### 21.6.1. Intrusion Detection System

To configure the Intrusion Detection System, follow these steps:

1. To turn on the Intrusion Detection System, click the corresponding switch.
2. Drag the slider along the scale to set the desired aggressiveness level. Use the description on the right side of the scale to choose the level that better fits your security needs.

You can check what applications have been detected by the Intrusion Detection System in the Events window.

If there are applications you trust and do not want the Intrusion Detection System to scan, you can add exclusion rules for them. To exclude an application from scanning, follow the steps described in section “*Managing excluded processes*” (p. 95).

Note

The operation of the Intrusion Detection System is related to that of the Active Virus Control. Process exclusion rules apply to both systems.

### 21.6.2. Other settings

The following features can be enabled or disabled.

- **Internet connection sharing** - enables support for Internet connection sharing.

  Note

  This option does not automatically enable **Internet connection sharing** on your system, but only allows this type of connection in case you enable it from your operating system.

- **Block port scans** - detects and blocks attempts to find out which ports are open.

  Port scans are frequently used by hackers to find out which ports are open on your computer. They might then break into your computer if they find a less secure or vulnerable port.

- **Increase log verbosity** - increases the verbosity of the Firewall log.

  Bitdefender maintains a log of events regarding the Firewall module usage (enabling/disabling firewall, traffic blocking, modifying settings) or generated by the activities detected by this module (scanning ports, blocking connection attempts or traffic according to the rules). The log can be accessed from the **Firewall Activity** window by clicking **Show Log**.

- **Monitor Wi-Fi connections** - when you are connected to wireless networks, information is displayed regarding specific network events (for example, when a new computer has joined the network).

# 22. Safepay security for online transactions

The computer is fast becoming the main tool for shopping and banking. Paying bills, transferring money, buying pretty much anything you can imagine has never been quicker or easier.

This involves sending personal information, account and credit card data, passwords and other types of private information over the Internet, in other words exactly the type of information flow that cyber-criminals are very interested to tap into. Hackers are relentless in their efforts to steal this information, so you can never be too careful about securing online transactions.

Bitdefender Safepay is first of all a protected browser, a sealed environment that is designed to keep your online banking, e-shopping and any other type of online transaction private and secure.

For the best privacy protection, Bitdefender Wallet has been integrated into Bitdefender Safepay to secure your credentials whenever you want to access private online locations. For more information, please refer to "*Wallet protection for your credentials*" (p. 138).

Bitdefender Safepay offers the following features:

- It blocks access to your desktop and any attempt to take snapshots of your screen.
- It protects your secret passwords while browsing online with Wallet.
- It comes with a virtual keyboard which, when used, makes it impossible for hackers to read your keystrokes.
- It is completely independent from your other browsers.
- It comes with built-in hotspot protection to be used when your computer is connected to unsecured Wi-fi networks.
- It supports bookmarks and allows you to navigate between your favorite banking/shopping sites.
- It is not limited to banking and e-shopping. Any website can be opened in Bitdefender Safepay.

## 22.1. Using Bitdefender Safepay

By default, Bitdefender detects when you navigate to an online banking site or online shop in any browser on your computer and prompts you to launch it in Bitdefender Safepay.

To access the main interface of Bitdefender Safepay, follow the steps below:

- In **Windows XP**, **Windows Vista** and **Windows 7**:
  1. Click **Start** and go to **All Programs**.

2. Click **Bitdefender**.
3. Click **Bitdefender Safepay** or, quicker, double-click the Bitdefender Safepay shortcut on your desktop.

- In **Windows 8**:

  Locate Bitdefender Safepay from the Windows Start screen (for example, you can start typing "Bitdefender Safepay" directly in the Start screen) and then click the icon. Alternatively, open the Desktop app and double-click the Bitdefender Safepay shortcut.

Note

If the Adobe Flash Player plugin is not installed or is outdated, a Bitdefender message will be displayed. Click the corresponding button to continue.
After the installation process is completed, you will have to manually reopen the Bitdefender Safepay browser to continue your work.

If you are used to web browsers, you will have no trouble using Bitdefender Safepay - it looks and behaves like a regular browser:

- enter URLs you want to go to in the address bar.
- add tabs to visit multiple websites in the Bitdefender Safepay window by clicking .
- navigate back and forward and refresh pages using respectively.
- access Bitdefender Safepay settings by clicking .
- protect your passwords with Wallet by clicking .
- manage your bookmarks by clicking next to the address bar.
- open the virtual keyboard by clicking .

## 22.2. Configuring settings

Click to configure the following settings:

**General Bitdefender Safepay behavior**

Choose what will happen when you access an online shop or Internet banking site in your regular web browser:

- Automatically open in Bitdefender Safepay.
- Have Bitdefender prompt you for action each time.
- Never use Bitdefender Safepay for pages visited in a regular browser.

**Domains list**

Choose how Bitdefender Safepay will behave when you visit websites from specific domains in your regular web browser by adding them to the domains list and selecting the behavior for each one:

- Automatically open in Bitdefender Safepay.
- Have Bitdefender prompt you for action each time.
- Never use Bitdefender Safepay when visiting a page from the domain in a regular browser.

## 22.3. Managing bookmarks

If you disabled the automatic detection of some or all websites, or Bitdefender simply doesn't detect certain websites, you can add bookmarks to Bitdefender Safepay so that you can easily launch favorite websites in the future.

Follow these steps to add a URL to Bitdefender Safepay bookmarks:

1. Click next to the address bar to open the Bookmarks page.

   Note
   The Bookmarks page is opened by default when you start Bitdefender Safepay.

2. Click the **+** button to add a new bookmark.
3. Enter the URL and the title of the bookmark and click **Create**. The URL is also added to the Domains list on the settings page.

## 22.4. Hotspot protection for unsecured networks

When using Bitdefender Safepay while connected to unsecured Wi-fi networks (for example, a public hotspot) an extra layer of security is offered by the Hotspot protection feature. This service encrypts Internet communication over unsecured connections, helping you maintain your privacy no matter what network you are connected to.

The following prerequisites must be met for Hotspot protection to work:

- You are logged in to a MyBitdefender account from Bitdefender Total Security.
- Your computer is connected to an unsecured network.

Once the prerequisites are met, Bitdefender will automatically prompt you to use the secured connection whenever you open Bitdefender Safepay. All you need to do is enter your MyBitdefender credentials when prompted.

The secure connection will be initialized and a message will be displayed in the Bitdefender Safepay window when the connection is established. The symbol

appears in front of the URL in the address bar to help you easily identify secure connections.

# 23. Wallet protection for your credentials

We use our computers to shop online or pay our bills, to connect to social media platforms or log in with instant messaging applications.

But as everybody knows, it's not always easy to remember the password!

And if we are not careful while browsing online, our private information, such as our e-mail address, our instant messaging ID or our credit card data can be compromised.

To keep your passwords or your personal data on a sheet of paper or in the computer can be dangerous because they can be accessed and used by people who want to steal and use that information. And to remember each password you have set for your online accounts or for your favorite websites is not an easy task.

Therefore, is there a way to make sure that we find our passwords when we need them? And can we rest assured that our secret passwords are always safe?

Wallet is the password manager that helps you keep track of your passwords, protects your privacy and provides a secure browsing experience.

Using a single master password to access your credentials, Wallet makes it easy for you to keep your passwords safe.

To offer the best protection for your online activities, Wallet is integrated with Bitdefender Safepay and provides a unified solution for the various ways in which your private data can be compromised.

Wallet protects the following private information:

- Personal information, such as the e-mail address or the phone number
- Login credentials for the websites
- Bank account information or the credit card number
- Access data to the e-mail accounts
- Passwords for the applications
- Passwords for the Wi-Fi networks

## 23.1. Configuring the Wallet

Once the installation is finished and you open your browser, you will be notified through a pop-up window that you can use Wallet for an easier browsing experience.

Click **Explore** to start the setup wizard for the Wallet. Follow the wizard to complete the setup process.

Two tasks can be performed during this step:

- Create a new Wallet database to protect your passwords.

During the setup process, you will be asked to protect your Wallet with a master password. The password should be strong and contain at least 7 characters.

To create a strong password use minimum one number or symbol, and one upper case character. Once you have set a password, anyone trying to access the Wallet will first have to provide the password.

At the end of the setup process, the following Wallet settings are enabled by default:

- **Save credentials automatically in Wallet**.
- **Ask for my master password when I login to my computer**.
- **Automatically lock Wallet when I leave my PC unattended**.

- Import an existing database if you previously used Wallet on your system.

## Export the Wallet database

To export your Wallet database, follow these steps:

1. Open the Bitdefender window.
2. On the **Wallet** panel, click **Manage** and select **Export Wallet** from the drop-down menu.
3. Follow the steps to export the Wallet database to a location on your system.

## Create a new Wallet database

To create a new Wallet database, follow these steps:

1. Open the Bitdefender window.
2. On the **Wallet** panel, click **Manage** and select **Create new Wallet** from the drop-down menu.
3. A warning window will appear informing you that the data currently stored in the Wallet will be deleted. Click **Yes** to wipe the existing database and to continue with the wizard. To exit the wizard, click **No**.

## Manage your Wallet credentials

To manage your passwords, follow these steps:

1. Open the Bitdefender window.
2. On the **Wallet** panel, click **Manage** and select **Open Wallet** from the drop-down menu.

A new window will appear. Select the desired category from the upper part of the window:

- My Info

- Websites
- Online banking
- Email client settings
- Apps and subscriptions
- Wi-Fi Networks

## Adding/ editing the passwords

- To add a new password, choose the desired category from the top, click **+ Add item**, insert the information in the corresponding fields and click the Save button.
- To edit an entry from the table, select it and click the **Edit** button.
- To exit, click **Cancel**.
- To remove an entry, select it, click the **Edit** button and choose **Delete**.

## 23.2. Turning on or off the Wallet protection

To turn the Wallet protection on or off, follow these steps:

1. Open the Bitdefender window.
2. On the **Wallet** panel, click the switch to turn on or off **Wallet**.

## 23.3. Managing the Wallet settings

To configure the master password in detail, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Wallet**.
4. In the **Wallet Settings** window, select the **Master password** tab.

The following options are available:

- **Ask for my master password when I login to my computer** - you will be prompted to insert your master password when you access the computer.
- **Ask for my master password when I open my browsers and apps** - you will be prompted to insert your master password when you access a browser or an application.
- **Automatically lock Wallet when I leave my PC unattended** - you will be prompted to insert your master password when you return to your computer after 15 minutes.

Important
Be sure to remember your master password or keep a record of it in a safe place. If you forget the password, you will have to reinstall the program or contact Bitdefender for support.

## Improve your experience

To select the browsers or the applications where you want to integrate the Wallet, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Wallet**.
4. In the **Wallet Settings** window, select the **Enhanced apps** tab.

   Check an application to use the Wallet and improve your experience:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Yahoo! Messenger
   - Skype

## Configuring the Autofill

The Autofill feature makes it easy for you to connect with your favorite websites or to log in with your online accounts. The first time you enter your credentials into your web browser, the Wallet saves the information automatically.

To configure the **Autofill** settings, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Wallet**.
4. In the **Wallet Settings** window, select the **Wallet Tweaks** tab.
5. Configure the following options:

   - **Autofill login credentials**:
     - **Autofill login credentials every time** - the credentials are inserted automatically into the browser.
     - **Ask for my master password before filling** - you need to provide the master password before having the credentials inserted into the browser.

- **Let me choose when I want to autofill my login credentials** - you can insert the credentials manually into the browser.

- **Configure how Wallet secures your logins**:
  - **Save credentials automatically in Wallet** - the login credentials are automatically saved and updated into the Wallet.
  - **Ask me every time** - you will be asked every time if you want to add your credentials to the Wallet.
  - **Do not save, I will update the information manually** - the credentials can be added only manually into the Wallet.

# 24. Parental Control

Parental Control enables you to control the access to the Internet and to specific applications for each user holding a user account on the system.

Once you have configured Parental Control, you can easily find out what your child is doing on the computer.

All you need is a computer with Internet access and a web browser.

You can configure Parental Control to block:

- inappropriate web pages.
- Internet access, for specific periods of time (such as when it's time for lessons).
- applications like games, chat, filesharing programs or others.
- instant messages sent by IM contacts other than those allowed.

Check your children's activities and change the Parental Control settings using MyBitdefender from any computer or mobile device connected to the Internet.

## 24.1. Accessing Parental Control dashboard

The Parental Control dashboard is organized into modules from where you can monitor the child's activities on the computer.

Bitdefender enables you to control the access to the Internet and to specific applications for your children. At the same time, it allows you to monitor their Facebook account activity.

With Bitdefender you can access Parental Control settings from MyBitdefender account on any computer or mobile device connected to the Internet.

Access your online account:

- On any device with Internet access:
  1. Open a web browser.
  2. Go to: https://my.bitdefender.com
  3. Log in to your account using your user name and password.
  4. Click **Parental Control** to access the dashboard.
- From your Bitdefender interface:
  1. Make sure you are logged on to the computer with an administrator account. Only users with administrative rights on the system (system administrators) can access and configure Parental Control.
  2. Open the Bitdefender window.
  3. Go to **Parental Control** panel and click the switch to turn it on.

4. Click the **Configure** button.

   Make sure that you are logged in to your MyBitdefender account.

5. The Parental Control dashboard will open in a new window. This is where you can check and configure the Parental Control settings of each Windows user account.

## 24.2. Adding your child's profile

Before you configure Parental Control, create separate Windows user accounts for your children to use. This will allow you to know exactly what each of them is doing on the computer. You should create limited (standard) user accounts so that they cannot change the Parental Control settings. For more information, please refer to "*How do I create Windows user accounts?*" (p. 57).

To add your child's profile to Parental Control:

1. Access the Parental Control dashboard from your MyBitdefender account.
2. Click **Add child** on the left-side menu.
3. Enter the name and age of the child in the corresponding fields. Setting the age of the child will automatically load settings considered appropriate for that age category, based on child development standards.
4. You can see below the devices that are linked to your MyBitdefender account.
5. Select the computer and the Windows account for your child.
6. Click **Create Profile**.

   The computer and the Windows account of your child are now linked to your MyBitdefender account.

### 24.2.1. Installing Parental Control on the Android device

To install Parental Control on your child's mobile device, follow these steps:

1. Access the Parental Control dashboard from your MyBitdefender account.
2. Click **Add child** on the left-side menu.
3. Enter the name and age of the child in the corresponding fields. Setting the age of the child will automatically load settings considered appropriate for that age category, based on child development standards.
4. Click **Install on new device** to continue.
5. A new window will appear. Select **Google Play** from the list.
6. To download and install Parental Control on the device, click the **Install** button.
7. Select the device where you want to install the app.

8. Click **Install** to continue.

   Wait for the app to install on the device. Make sure the child's device is connected to the Internet.

9. At the end of the installation, you will be prompted to give the application administrator rights on the device.

10. Tap **Accept** to finish the installation.

### Linking Parental Control to MyBitdefender

To monitor your child's online activity, you must link the child's device to your MyBitdefender account by logging in to the account from the app.

To link the device to your MyBitdefender account, follow these steps:

1. Enter your MyBitdefender user name and password.

   If you do not have an account, choose to create a new account using the corresponding button.

   **Note**
   You may also enter a name for your device. If you link more than one device to your account, this will help you identify the devices more easily.

2. Tap **Sign-in**.

   Your child's device is now linked to your MyBitdefender account and you can start monitoring his online activities.

## 24.2.2. Monitoring the child's activity

Bitdefender helps you keep track of what your children are doing online.

In this way, you can always find out exactly what websites they have visited, what applications they have used or what activities have been blocked by the Parental Control.

The reports contain detailed information for each event, such as:

- The status of the event.
- The name of the blocked website.
- The name of the blocked application.
- The device name.
- The date and time when the event occurred.
- The actions taken by Bitdefender.

To monitor the Internet traffic, the accessed applications or the Facebook activity for your child, follow these steps:

1. Access the Parental Control dashboard from your MyBitdefender account.
2. Click to access the activity window for the corresponding module.

### 24.2.3. Configuring the General Settings

By default, when Parental Control is enabled, your children's activities are logged.

To receive e-mail notifications, follow these steps:

1. Access the Parental Control dashboard from your MyBitdefender account.
2. Click the **General Settings** icon on the top right corner.
3. Enable the option to receive activity reports.
4. Enter the e-mail address where the e-mail notifications are to be sent.
5. Adjust the frequency by selecting: daily, weekly or monthly.
6. Receive e-mail notifications for the following:
   - Blocked websites
   - Blocked apps
   - Blocked IM contact
   - SMS from a blocked contact
   - Call received from a blocked phone number
   - Removal of Parental Control Facebook app
7. Click **Save**.

Take a look at the **Account info** area. You can see the registration status, the current license key and the expiration date.

## 24.3. Configuring Parental Control

The Parental Control dashboard is where you can directly manage the Parental Control modules.

Each module contains the following elements: the name of the module, a status message, the icon of the module and a button that lets you perform important tasks related to the module.

Click a tab to configure the corresponding Parental Control feature for the computer:

- Web - to filter web navigation and set time restrictions on Internet access.

- Applications - to block or restrict access to specific applications.
- Facebook - to protect your child's Facebook account.
- Instant Messaging - to allow or block chat with specific instant messaging contacts.

The following modules can be accessed to monitor the child's activity on the mobile device:

- Location - to find the current location of your child's device on Google Maps.
- SMS - to block incoming text messages from a phone number.
- Calls - to block calls from a phone number, both incoming and outgoing.

### 24.3.1. Web Control

Web control helps you block websites with inappropriate content and set time restrictions on Internet access.

To configure Web control for a specific user account:

1. Go to the **Web** tab.
2. Click on the **Web** panel to access the **Web Activity** window.
3. Use the switch to turn on **Web Activity**.

#### Allowing or blocking a website

Use the **Web Activity** window to see all the web pages accessed by your child.

- To block access to a website, follow these steps:
  1. Click the **Blacklist** button.
  2. Enter the website in the corresponding field.
  3. Click **Add** to add the website to the list.
  4. Select from the grid the time intervals during which access is allowed. You can click individual cells, or you can click and drag to cover longer periods.

     Click the **Save** button.
  5. If you change your mind, select the website and click the corresponding **Remove** button.
- To allow access to a blocked website, follow these steps:
  1. Click the **Blacklist** button.
  2. Enter the website in the corresponding field.
  3. Click **Add** to add the website to the list.

4. Select from the grid the time intervals during which access is allowed. You can click individual cells, or you can click and drag to cover longer periods.

   Click the **Save** button.

5. If you change your mind, select the website and click the corresponding **Remove** button.

## Keywords control

Keywords control helps you block users' access to instant messages and web pages that contain specific words. Using Keywords control you can prevent your children from seeing inappropriate words or phrases when they are online. Furthermore, you can ensure they will not be giving out personal information (such as the home address or phone number) to people they met on the Internet.

To configure Keywords control for a specific user account, follow these steps:

1. Click the **Keywords** button.
2. Enter the keyword in the corresponding field.
3. Click **Block** to add the word to the list of banned keywords. If you change your mind, click the corresponding **Remove** button.

## Category filter

The Category filter dynamically filters access to websites based on their content. When you set the age of your child, the filter is automatically configured to block website categories considered inappropriate for your child's age. This configuration is suitable in most cases.

If you want more control over the Internet content your child is exposed to, you can choose the specific website categories to be blocked by the Category filter.

To configure in detail the Category filter settings for a specific user account, follow these steps:

1. Click the **Categories** button.
2. You can check what web categories are automatically blocked / restricted for the currently selected age group. If you are not satisfied with the default settings, you can configure them as needed.
3. Click **Save**. If you change your mind, click the **Reset** button to use default level of protection based on your child's age.

## Restricting Internet access by time

You can specify when your child is allowed to access the Internet using the **Schedule** option in the **Web Activity** window.

To configure in detail the Internet access for a specific user account, follow these steps:

1. Click the **Schedule** button.
2. Select from the grid the time intervals during which Internet access is blocked. You can click individual cells, or you can click and drag to cover longer periods.
3. Click the **Save** button.

### 24.3.2. Applications Control

The Application control helps you to block any application from running. Games, media and messaging software, as well as other categories of software and malware can be blocked this way.

To configure Application control for a specific user account, follow these steps:

1. Go to the **Applications** tab.
2. Click on the **Applications** panel to access the **Application Activity** window.
3. Use the switch to turn on **Application Activity**.
4. Click the **Blacklist** button.
5. Enter the name of the application:
   - To block an app for a mobile device, select the apps you want to block from the **Allowed apps** list.
   - To block an application in the Windows operating system, add the executable file of the application you want to block (.exe).
6. Click **Block** to add the application to the **Blocked apps** list or **Allow** to add the application to the **Allowed apps** list.

### 24.3.3. Facebook protection

Parental Control monitors your child's Facebook account and reports the main activities taking place.

These online activities are verified and you are warned if they prove to be a threat for your account privacy.

The monitored elements of the online account include:

- the number of friends
- comments of the child or his friends on his photos or posts
- messages
- wall posts

- uploaded photos and videos
- account privacy settings

To configure Facebook protection for a specific user account:

1. Go to the **Facebook** tab.
2. Click **Connect child's profile** in the **Facebook** panel.
3. To protect the child's Facebook account, install the application using the corresponding link.

Note
To install the application you will need the credentials of your child's Facebook profile.

To stop monitoring the Facebook account, use the **Unlink account** button from the top.

### 24.3.4. Instant Messaging control

The Instant Messaging (IM) control allows you to specify the IM contacts your children are allowed to chat with or block access to instant messages that contain specific words.

Note
The IM Control is only available for Yahoo! Messenger and Windows Live (MSN) Messenger.

To configure Instant Messaging control for a specific user account, follow these steps:

1. Go to the **Instant Messaging** tab.
2. Click on the **Instant Messaging** panel to access the **Instant Messaging Activity** window.
3. Use the switch to turn on **Instant Messaging Activity**.

   Restrict the **Instant Messaging** access using one of the available options:

   - **Blacklist** button to enter the e-mail address associated with the instant messaging ID.
   - **Keywords** button to block access to instant messages that contain specific words.

### 24.3.5. Location

View the device's current location on Google Maps. The location is refreshed every 5 seconds, so you can track it if it is on the move.

The accuracy of the location depends on how Bitdefender is able to determine it:

- If the GPS is enabled on the device, its location can be pinpointed to within a couple of meters as long it is in the range of GPS satellites (i.e. not inside a building).
- If the device is indoors, its location can be determined to within tens of meters if Wi-Fi is enabled and there are wireless networks available in its range.
- Otherwise, the location will be determined using only information from the mobile network, which can offer an accuracy no better than several hundred meters.

Note

For the **Remote geolocation** to be accurate, make sure you have enabled the GPS, the Wi-Fi or the mobile network connection on the mobile device.

### 24.3.6. Text messages control

The Text messages control helps you stop receiving text messages associated with a phone number.

- To block text messages received from a phone number, follow these steps:
  1. Go to the **SMS** tab.
  2. Click on the **SMS** panel to access the **SMS Activity** window.
  3. Use the switch to turn on **SMS Activity**.
  4. Click the **Blacklist** button.
  5. Add a phone number in the corresponding field.
  6. Click **Block** to add the phone number to the blacklist. The phone number will be added to the list of blocked phone numbers.
- To allow receiving text messages from a blocked phone number, follow these steps:
  1. Click the **Blacklist** button at the top.
  2. Select the phone number from the list.
  3. Click **Remove**. The phone number will be removed from the list of blocked phone numbers.

Note
Make sure you use the specific country code when you insert the phone number in the list.

### 24.3.7. Phone numbers control

The Phone numbers control helps you stop sending or receiving calls associated with a phone number.

- To block sending or receiving calls associated with a phone number, follow these steps:
  1. Go to the **Calls** tab.
  2. Click on the **Calls** panel to access the **Call Activity** window.
  3. Use the switch to turn on **Call Activity**.
  4. Click the **Blacklist** button.
  5. Add a phone number in the corresponding field.
  6. Click **Block** to add the phone number to the blacklist. The phone number will be added to the list of blocked phone numbers.
- To allow calls to a blocked phone number, follow these steps:
  1. Click the **Blacklist** button at the top.
  2. Select the phone number from the list.
  3. Click **Remove**. The phone number will be removed from the list of blocked phone numbers.

Note
Make sure you use the specific country code when you insert the phone number in the list.

# 25. Safego protection for Facebook

You trust your online friends, but do you trust their computers? Use Safego protection for Facebook to protect your account and your friends from online threats.

Safego is a Bitdefender application developed to keep your Facebook account safe. Its role is to scan the links you receive from your friends and monitor your account privacy settings.

Note
A MyBitdefender account is required in order to use this feature.
For more information, please refer to "*MyBitdefender account*" (p. 35).

These are the main features available for your Facebook account:

- automatically scans the posts in your News Feed for malicious links.
- protects your account against online threats.

  When it detects a post or a comment which is a spam, a phishing or a malware, you will receive a warning message.
- warns your friends on suspicious links posted on their News Feed.
- helps you build a safe network of friends using the **Friend'O'Meter** feature.
- get a system safety status check provided by Bitdefender QuickScan.

To access Safego for Facebook, follow these steps:

- From the Bitdefender interface:
  1. Open the Bitdefender window.
  2. On the **Safego** panel, click **Manage** and select **Activate for Facebook** from the drop-down menu.

     You will be directed to your account.
  3. Use your Facebook login information to connect to the Safego application.
  4. Allow Safego access to your Facebook account.

  If Safego has already been activated, you will be able to access statistics regarding its activity by selecting **Reports for Facebook** in the menu.
- From MyBitdefender account:
  1. Go to: https://my.bitdefender.com.
  2. Log in to your account using your user name and password.
  3. Click **Facebook Protection**.

     A message informing you that Facebook protection is not activated for your account is displayed.

4. Click **Activate** in order to continue.
   You will be directed to your account.
5. Use your Facebook login information to connect to the Safego application.
6. Allow Safego access to your Facebook account.

# 26. Device Anti-Theft

Laptop theft is a major issue that affects individuals and organizations alike. Even more than losing the hardware itself, the data lost with it can cause significant damage, both financially and emotionally.

Yet few people take the proper steps to secure their important personal, business and financial data in the case of theft or loss.

Bitdefender Anti-Theft helps you be better prepared for such an event by allowing you to remotely locate or lock your computer and even wipe all data from it, should you ever part with your computer against your will.

To use the Anti-Theft features, the following prerequisites must be met:

- You must link your computer to a MyBitdefender account by logging into one from Bitdefender Total Security.
- The commands can only be sent from the MyBitdefender account you linked your computer to.
- The computer must be connected to the Internet to receive the commands.

Anti-Theft features work in the following way:

**Remote Locate**

View your device's location on Google Maps.

The accuracy of the location depends on how Bitdefender is able to determine it. The location is determined to within tens of meters if Wi-fi is enabled on your computer and there are wireless networks in its range.

If the computer is connected to a wired LAN with no Wi-fi based location available, the location will be determined based on the IP address, which is considerably less accurate.

**Remote Lock**

Lock your computer and set a 4 digit PIN for unlocking it. When you send the Lock command, the computer reboots and logging back into Windows is only possible after entering the PIN you have set.

**Remote Wipe**

Remove all data from your computer. When you send the Wipe command, the computer reboots and the data on all hard drive partitions is erased.

Anti-Theft is activated after the installation and can be accessed exclusively through your MyBitdefender account from any device connected to the Internet, anywhere.

## Using Anti-Theft features from MyBitdefender

To access the Anti-Theft features from your account, follow these steps:

1. Go to https://my.bitdefender.com and log in to your account.
2. Click **Anti-Theft**.
3. Select your computer from the list of devices.
4. Select the feature you want to use:

   **Locate** - display your device's location on Google Maps.

   **Wipe** - delete all data from your computer.

   Important
   After you wipe a device, all Anti-Theft features cease to function.

   **Lock** - lock your computer and set a PIN code for unlocking it.

# 27. USB Immunizer

The Autorun feature built into Windows operating systems is a very useful tool that allows computers to automatically execute a file from media connected to it. For example, software installations can start automatically when a CD is inserted into the optical drive.

Unfortunately, this feature can also be used by malware to automatically launch and infiltrate your computer from rewritable media such as USB flash drives and memory cards connected through card readers. Numerous Autorun based attacks have been created in recent years.

With USB Immunizer you can prevent any NTFS, FAT32 or FAT formatted flash drive from automatically executing malware ever again. Once an USB device is immunized, malware can no longer configure it to run a certain application when the device is connected to a computer running Windows.

To immunize an USB device, follow these steps:

1. Connect the flash drive to your computer.
2. Browse your computer to locate the removable storage device and right-click its icon.
3. In the contextual menu, point to **Bitdefender** and select **Immunize this drive**.

Note

If the drive has already been immunized, the message **The USB device is protected against autorun-based malware** will appear instead of the Immunize option.

To prevent your computer from launching malware from unimmunized USB devices, disable the media autorun feature. For more information, please refer to *"Using automatic vulnerability monitoring"* (p. 97).

# 28. Managing your computers remotely

Your MyBitdefender account allows you to manage the Bitdefender products installed on your computers remotely.

Use MyBitdefender to create and apply tasks to your computers from a remote location.

Any computer will be managed from MyBitdefender account if it meets the following conditions:

- you have installed Bitdefender Total Security product on the computer
- you have linked the Bitdefender product to the MyBitdefender account.
- the computer is connected to the Internet

## 28.1. Accessing MyBitdefender

Bitdefender enables you to control the security of your computers by adding tasks to your Bitdefender products.

With Bitdefender you can access your MyBitdefender account on any computer or mobile device connected to the Internet.

Access MyBitdefender:

- On any device with Internet access:
  1. Open a web browser.
  2. Go to: https://my.bitdefender.com
  3. Log in to your account using your user name and password.
- From your Bitdefender interface:
  1. Open the Bitdefender window.
  2. Click the **MyBitdefender** button at the top of the window and select **Dashboard** from the drop-down menu.

## 28.2. Running tasks on the computers

To run a task on one of your computers, access your MyBitdefender account.

If you click a computer icon at the bottom of the window, you can see all the administrative tasks you can run on the remote computer.

**Product registration**
Allows you to register Bitdefender on the remote computer by entering a license key.

**Perform a complete scan of your PC**
Allows you to run a complete scan on the remote computer.

**Scan critical areas to detect active malware**
Allows you to run a quick scan on the remote computer.

**Fix critical issues**
Allows you to fix the issues that are affecting the security of the remote computer.

**Product update**
Initiates the update process for the Bitdefender product installed on this computer.

# Tune-up and backup

# 29. Tune-Up

Bitdefender comes with a Tune-Up module that helps you maintain the integrity of your system. The maintenance tools offered are critical for the improvement of your system's responsiveness and the efficient management of the hard drive space.

Bitdefender provides the following PC tune-up tools:

- PC Clean-Up removes the temporary Internet files and cookies, unused system files and recent documents shortcuts.
- Disk Defragmenter physically reorganizes the data on the hard disk so that the pieces of each file are stored close together and continuously.
- Duplicate Finder finds and deletes files that are duplicated in your system.
- Registry Cleaner identifies and deletes invalid or outdated references in the Windows Registry. In order to keep the Windows Registry clean and optimized, it is recommended to run the Registry Cleaner monthly.
- Registry Recovery can retrieve registry keys previously deleted from the Windows Registry using Bitdefender Registry Cleaner.
- Performance Monitor monitors your system hardware and software configuration in order to make sure you are fully protected from malware.

## 29.1. Cleaning up your PC

Every time you visit a web page, temporary Internet files are created in order to allow you to access it quicker next time.

Cookies are also stored on your computer when you visit a web page.

The PC Clean-up wizard helps you free disk space and protect your privacy by deleting files that may no longer be useful.

- Internet Explorer temporary Internet files and cookies.
- Mozilla Firefox temporary Internet files and cookies.
- temporary system files Windows creates during its operation.
- recent documents shortcuts Windows creates when you open a file.

To start the PC Clean-Up wizard, follow these steps:

1. Open the Bitdefender window.
2. On the **Tune-Up** panel, click **Optimize** and select **PC Clean-Up** from the drop-down menu.
3. Follow the three-step guided procedure to perform the clean-up. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.

a. **Welcome**

Turn on or off the PC Clean-Up options by clicking **Custom Clean**:

- Clean Internet Explorer cache
- Clean Mozilla Firefox cache
- Clean Recent Documents List and Temporary System Files

b. **Perform Cleaning**

c. **Results**

## 29.2. Defragmenting hard disk volumes

When copying a file exceeding the largest block of free space on the hard disk, file fragmentation occurs. Because there is not enough free space to store the entire file continuously, it will be stored in several blocks. When the fragmented file is accessed, its data must be read from several different locations.

It is recommended to defragment the hard disk in order to:

- access files faster.
- improve overall system performance.
- extend hard disk life.

To start the Disk Defragmenter wizard, follow these steps:

1. Open the Bitdefender window.
2. On the **Tune-Up** panel, click **Optimize** and select **Disk Defragmenter** from the drop-down menu.
3. Follow the five-step guided procedure to perform the defragmentation. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.

   a. **Choose disks to analyze**

   Select the partitions you want to check for fragmentation.

   b. **Analyzing selected partitions**

   Wait for Bitdefender to finish analyzing the partitions.

   c. **Select disk**

   The fragmentation status of the analyzed partitions is displayed. Select the partitions you want to be defragmented.

   d. **Defragmenting**

   Wait for Bitdefender to finish defragmenting the partitions.

   e. **Results**

Note
Defragmentation may take a while since it involves moving portions of stored data from a place to another on the hard disk. We recommend you to perform defragmentation when you are not using your computer.

## 29.3. Finding duplicate files

Duplicate files eat up your hard disk space. Just think about having the same `.mp3` file stored in three different locations.

The Duplicate Finder wizard will help you detect and delete duplicate files on your computer.

To start the Duplicate Finder wizard, follow these steps:

1. Open the Bitdefender window.
2. On the **Tune-Up** panel, click **Optimize** and select **Duplicate Finder** from the drop-down menu.
3. Follow the four-step guided procedure to identify and remove duplicates. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.
   a. **Select target**

      Add the folders where to search for duplicate files.

   b. **Search for duplicates**

      Wait for Bitdefender to finish searching for duplicates.

   c. **Select files for deletion**

      Identical files are listed in groups. You can choose an action to take on all groups or on each separate group: keep newest, keep oldest or take no action. You can also select actions for each individual file.

      Note
      If no duplicated files are found, this step will be skipped.

   d. **Results**

## 29.4. Cleaning Windows registry

Many applications write keys in the Windows Registry at installation time. When removing such applications, some of their associated registry keys might not be deleted and continue to remain in the Windows Registry, slowing down your system and even causing system instability. The same happens when you delete shortcuts to or certain files of applications installed on your system, as well as in the case of corrupt drivers.

To start the Registry Cleaner wizard, follow these steps:

1. Open the Bitdefender window.
2. On the **Tune-Up** panel, click **Optimize** and select **Registry Cleaner** from the drop-down menu.
3. Follow the four-step guided procedure to clean the registry. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.
   a. **Welcome**
   b. **Perform Scan**

      Wait for Bitdefender to finish scanning the registry.
   c. **Select Keys**

      You can see all the invalid or orphan registry keys detected. Detailed information is provided about each registry key (name, value, priority, category).

      The registry keys are grouped based on their location in the Windows Registry:

      - **Software Locations.** Registry keys that contain information about the path to applications installed on your computer.

        The invalid keys are assigned a low priority, which means that you can delete them without almost any risk.
      - **Custom Controls.** Registry keys that contain information about the file extensions registered on your computer. These registry keys are commonly used to maintain file associations (to ensure that the correct program opens when you open a file using Windows Explorer). For example, such a registry key allows Windows to open a `.doc` file in Microsoft Word.

        The invalid keys are assigned a low priority, which means that you can delete them without almost any risk.
      - **Shared DLLs.** Registry keys that contain information on the location of shared DLLs (Dynamic Link Libraries). DLLs store functions that are used by installed applications to perform certain tasks. They can be shared by multiple applications to reduce memory and disk space requirements.

        These registry keys become invalid when the DLL they point to is moved to another location or completely removed (this usually happens when you uninstall a program).

        The invalid keys are assigned a medium priority, which means that deleting them may negatively affect the system.

      By default, all the keys are marked for deletion. You can choose to delete individual invalid keys from a selected category.
   d. **Results**

## 29.5. Recovering cleaned registry

Sometimes, after registry clean up, you might notice that your system does not work well or that some applications fail to operate properly due to missing registry keys. This may be caused by shared registry keys that were deleted during registry cleaning or by other deleted keys. To solve this problem, you must recover the cleaned registry.

To start the Registry Recovery wizard, follow these steps:

1. Open the Bitdefender window.
2. On the **Tune-Up** panel, click **Optimize** and select **Registry Recovery** from the drop-down menu.
3. Follow the two-step guided procedure to recover the cleaned registry. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.

   a. **Select checkpoint**

   You can see a list of time points when the Windows Registry was cleaned. Select the time point to restore the Windows Registry to.

   Warning
   The recovery of the cleaned registry might overwrite the registry keys edited since the last registry clean up.

   b. **Task results**

## 29.6. Performance Monitor

The Performance Monitor module constantly monitors the system load, allowing you to see the running applications and the impact they have on the general behavior of the system.

These are its main functions:

- To present the system CPU and memory usage by using a set of indicators.
- To determine the applications resource usage.
- To help you close any high resource usage application which causes the system to perform poorly.

To access the Performance Monitor options, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Tune-Up**.

4. In case you encounter a slow down issue, the problem may be caused by some applications running on your system. To solve the problem, follow these steps:
   a. Identify the application which causes the issue.
   b. Click the application name to view a history of the CPU and memory usage and also the installation path.
   c. Close the application by using the provided button.

Warning
If you suspect the application (or the process) you want to close is part of the Windows operating system and your action could affect the system, contact Bitdefender for support as described in section “*Asking for help*” (p. 201).

# 30. Safebox online backup and sync

Safebox is the Bitdefender service that allows you to back up your important data on secure online servers, share it with your friends and synchronize it between your devices.

Note
A MyBitdefender account is required in order to use this feature.
For more information, please refer to "*MyBitdefender account*" (p. 35).

With Safebox:

- You get 2GB of free online space for your backups.
- You can manage your backups directly from Windows Explorer. For more information, please refer to Managing Safebox backups from Windows.
- Previously backed up files that have been deleted can be restored.
- Changes made to your files are saved so that you can recover previous versions.
- You can synchronize files between multiple devices running Bitdefender Total Security or the standalone Safebox application. Safebox applications are available for Windows PC, iOS and Android.

  For more information, visit http://www.bitdefender.com/solutions/safebox.html.
- You can access your files even on devices on which Bitdefender Total Security or Bitdefender Safebox are not installed by simply accessing your MyBitdefender account straight from the browser of any computer or mobile device connected to the Internet.

## 30.1. Activating Safebox

To activate Safebox, follow these steps:

1. Open the Bitdefender window.
2. On the **Safebox** panel, click the **Auto Sync** switch.

For a seamless backup of your data to the Bitdefender servers, keep automatic synchronization on.

Safebox backups can be managed from the Bitdefender window, from Windows Explorer and other file managers using the Windows contextual menu, or online from the MyBitdefender account.

## 30.2. Managing Safebox from the Bitdefender window

To manage your Safebox backups from Bitdefender, follow these steps:

1. Open the Bitdefender window.

2. On the **Safebox** panel, click **Manage** and select an option from the drop-down menu.

**Manage folders**

A new window will appear listing the folders added to Safebox from this computer, as well as from other computers or from MyBitdefender.

- To add a new folder to Safebox sync, browse to it on your computer, drag and drop it in the Manage Folders window.

  Add folders to Safebox sync and enable Safebox Auto Sync to automatically synchronize their contents with the Safebox online servers available from MyBitdefender.

- To remove a folder from Safebox sync, select it and click the **Unsync** button.

  Note
  Removing a folder from Safebox sync does not delete the online folder, it only removes the link between the local folder and the online folder.

- Safebox folders added from other computers or from MyBitdefender appear in the list but are not synced by default (the icon appears next to them).

  To add one such folder to the synced folders on this computer, select it and click **Sync**. A new window will appear prompting you to select the location of the local folder. Click **Yes** to use the default location, or **No** to select a different location.

  To remove an unsynced folder added from another computer from the list, select it and click **Delete**.

**Manage shared files**

A new window will appear listing the files added to Safebox sharing from this computer, as well as from other computers or from MyBitdefender.

- To add a new file to Safebox sharing, browse to it on your computer, drag and drop it in the Manage Sharing window. A new window will appear showing the upload progress. Once the upload is completed, copy the public link to the clipboard by clicking the corresponding message.
- To copy the link of a file from the list to the clipboard, click the **Share link** button and then click the corresponding message.
- To remove a file from Safebox sharing, select it and click **Delete link**.

## 30.3. Managing Safebox from Windows

Whenever you right-click a folder or inside a folder, the Windows contextual menu will give you quick access to all available Safebox operations.

### 30.3.1. Adding folders to Safebox

To add a folder to Safebox, right-click its icon or anywhere inside the folder and select **Add to Safebox**.

A remote folder is created on Bitdefender servers and the entire folder contents are uploaded to it. When the folder synchronization is completed, the Bitdefender icon will appear over the folder icon.

The icons of the files and folders in a Safebox folder will change according to the status of their synchronization with the remote folder:

The file / folder is synchronized.

The file / folder is not synchronized.

The file / folder is being synchronized.

Once a folder is added to Safebox and as long as Auto Sync is on, the folder contents are automatically synced with the online (remote) folder.

### 30.3.2. Removing folders from Safebox

To remove a folder from Safebox sync, right-click it, point to **Bitdefender Safebox** and select **Remove from Bitdefender Safebox**. A confirmation window will appear. Click **Yes** to stop Safebox from syncing the folder.

### 30.3.3. Restoring files deleted from Safebox

Once a folder is added to Safebox, Bitdefender keeps track of all the modifications made in that folder. This allows you to restore files deleted from a local Safebox folder and to recover previous versions of files you modified over time.

To restore the files that were deleted from a Safebox folder, right-click the folder icon or anywhere inside the folder, point to **Bitdefender Safebox** and select **Restore deleted files**. This will restore the latest versions of all the files deleted from the folder.

To restore a single file to a certain version, follow these steps:

1. Right-click the file.
2. Point to **Bitdefender Safebox** and select **View previous versions**.
3. A list of points in time when the file was modified is displayed. Select the version you want to restore.
4. Click **Recover to...**.
5. Select the folder where you want to restore the file and click **OK**.

## 30.4. Managing Safebox from MyBitdefender

You can access your Safebox folders through your MyBitdefender account from any computer or mobile device connected to the Internet. The same operations can be performed from your account as from Bitdefender Total Security.

To access Safebox from MyBitdefender:

- From any computer or mobile device, log in to your account at https://my.bitdefender.com and then click the Safebox icon.
- From Bitdefender Total Security:
  1. Open the Bitdefender window.
  2. On the **Safebox** panel, click **Manage** and select **Go to Dashboard** from the drop-down menu.

## 30.5. Synchronizing files between your computers

File synchronization between two or more computers works when the following conditions are met:

- Bitdefender Total Security or the standalone Safebox application is installed on the computers between which you want to sync files.
- You are logged in with the same MyBitdefender account on each computer.
- Local folders linked to the same online folder have been added to Safebox sync on each computer.
- For automatic synchronization, make sure Safebox **Auto Sync** is enabled on each computer.

If the conditions are met, the contents of folders added to Safebox on one computer will be synchronized with those linked to the same remote folders on the other computers.

## 30.6. Upgrading your online space

Safebox offers you 2GB of free online space for your backups.

In case you have a large amount of data that includes music, movies or important files that need to be protected, the 2GB of free online space may not be enough.

To upgrade your Safebox space, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Safebox**.
4. In the **Safebox Settings** window, click **Upgrade Safebox**.

5. The MyBitdefender page will open in your web browser. Follow the instructions to purchase additional space.

## 30.7. Removing files permanently

To completely remove a file from Safebox, you must remove it not just from the Safebox folder on your computer, but also from the online folder. Follow these steps:

1. Go to https://my.bitdefender.com and log in to your account.
2. Click the Safebox icon.
3. In the **Files and Folders** tab, select the file and then select **Delete** from the Actions drop-down menu. The file will be moved to the Safebox Recycle Bin.
4. In the **Recycle Bin** tab, select the file and then select **Remove** from the Actions drop-down menu. Click **Yes** in the confirmation window to completely delete the file.

Once a file is completely removed from Safebox, you can no longer restore it or recover older versions.

## 30.8. Limit bandwidth allocation

Backing up your files can put a strain on your Internet connection, especially when transferring large amounts of data.

In order not to interfere with your other online activities, you can limit the amount of bandwidth allocated to Safebox transfers.

To limit Safebox's bandwidth to 50 kB/s, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Safebox**.
4. In the **Safebox Settings** window, click the **Limit bandwidth** switch.

# Troubleshooting

# 31. Solving common issues

This chapter presents some problems you may encounter when using Bitdefender and provides you with possible solutions to these problems. Most of these problems can be solved through the appropriate configuration of the product settings.


- "*My system appears to be slow*" (p. 173)
- "*Scan doesn't start*" (p. 175)
- "*I can no longer use an application*" (p. 176)
- "*I cannot connect to the Internet*" (p. 177)
- "*I cannot access a device on my network*" (p. 178)
- "*My Internet is slow*" (p. 180)
- "*How to update Bitdefender on a slow Internet connection*" (p. 181)
- "*My computer is not connected to the Internet. How do I update Bitdefender?*" (p. 181)
- "*Bitdefender services are not responding*" (p. 182)
- "*Antispam filter does not work properly*" (p. 182)
- "*The Autofill feature in my Wallet doesn't work*" (p. 187)
- "*Bitdefender removal failed*" (p. 188)
- "*My system doesn't boot up after installing Bitdefender*" (p. 189)


If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the Bitdefender technical support representatives as presented in chapter "*Asking for help*" (p. 201).

## 31.1. My system appears to be slow

Usually, after installing a security software, there may appear a slight slowdown of the system, which to a certain degree is normal.

If you notice a significant slowdown, this issue can appear for the following reasons:

- **Bitdefender is not the only security program installed on the system.**

  Though Bitdefender searches and removes the security programs found during the installation, it is recommended to remove any other antivirus program you may use before installing Bitdefender. For more information, please refer to "*How do I remove other security solutions?*" (p. 72).

- **The Minimum System Requirements for running Bitdefender are not met.**

  If your machine does not meet the Minimum System Requirements, the computer will become sluggish, especially when multiple applications are running at the

same time. For more information, please refer to "*Minimum system requirements*" (p. 3).

- **There are too many invalid registry keys left in your Windows Registry.**

  Cleaning the Windows Registry can improve the performance of your system. For more information, please refer to "*Cleaning Windows registry*" (p. 163).

- **Your hard disk drives are too fragmented.**

  File fragmentation slows down file access and decreases system performance.

  Running the Disk Defragmenter can improve the performance of your system. For more information, please refer to "*Defragmenting hard disk volumes*" (p. 162).

- **The applications running on your system are using too many resources.**

  The Bitdefender Performance Monitor allows you to determine the impact of the applications running on your system by means of CPU load, memory usage and hard disk use.

  You should be able to pinpoint the applications that are causing the system to perform poorly, and close or monitor them. For more information, please refer to "*Performance Monitor*" (p. 165).

- **You have installed applications that you do not use**.

  Any computer has programs or applications that you do not use. And many unwanted programs run in the background taking up disk space and memory. If you do not use a program, uninstall it. This is also valid for any other pre-installed software or trial application you forgot to remove.

  Important

  If you suspect a program or an application to be an essential part of your operating system, do not remove it and contact Bitdefender Customer Care for assistance.

- **Your system may be infected**.

  Your system speed and its general behavior can also be affected by malware. Spyware, viruses, Trojans and adware all take a toll on your computer's performance. Make sure to scan your system periodically, at least once a week. It is recommended to use the Bitdefender System Scan because it scans for all types of malware threatening the security of your system.

  To start the System Scan, follow these steps:

  1. Open the Bitdefender window.
  2. On the **Antivirus** panel, click **Scan now** and select **System Scan** from the drop-down menu.
  3. Follow the wizard steps.

## 31.2. Scan doesn't start

This type of issue can have two main causes:

- **A previous Bitdefender installation which was not completely removed or a faulty Bitdefender installation**.

  In this case, follow these steps:

  1. Remove Bitdefender completely from the system:
     - In **Windows XP**:
       a. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.
       b. Wait a few moments until the list of installed software is displayed.
       c. Find **Bitdefender** and select **Remove**.
       d. Click **Remove** and then **Reinstall/change my Bitdefender product**.
       e. Wait for the uninstall process to complete and then reboot your system.
     - In **Windows Vista** and **Windows 7**:
       a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
       b. Wait a few moments until the installed software list is displayed.
       c. Find **Bitdefender** and select **Uninstall**.
       d. Click **Remove** and then **Reinstall/change my Bitdefender product**.
       e. Wait for the uninstall process to complete and then reboot your system.
     - In **Windows 8**:
       a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
       b. Click **Uninstall a program** or **Programs and Features**.
       c. Wait a few moments until the installed software list is displayed.
       d. Find **Bitdefender** and select **Uninstall**.
       e. Click **Remove** and then **Reinstall/change my Bitdefender product**.
       f. Wait for the uninstall process to complete and then reboot your system.
  2. Reinstall your Bitdefender product.

- **Bitdefender is not the only security solution installed on your system**.

  In this case, follow these steps:

1. Remove the other security solution. For more information, please refer to "*How do I remove other security solutions?*" (p. 72).
2. Remove Bitdefender completely from the system:
   - In **Windows XP**:
     a. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.
     b. Wait a few moments until the list of installed software is displayed.
     c. Find **Bitdefender** and select **Remove**.
     d. Click **Remove** and then **Reinstall/change my Bitdefender product**.
     e. Wait for the uninstall process to complete and then reboot your system.
   - In **Windows Vista** and **Windows 7**:
     a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
     b. Wait a few moments until the installed software list is displayed.
     c. Find **Bitdefender** and select **Uninstall**.
     d. Click **Remove** and then **Reinstall/change my Bitdefender product**.
     e. Wait for the uninstall process to complete and then reboot your system.
   - In **Windows 8**:
     a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
     b. Click **Uninstall a program** or **Programs and Features**.
     c. Wait a few moments until the installed software list is displayed.
     d. Find **Bitdefender** and select **Uninstall**.
     e. Click **Remove** and then **Reinstall/change my Bitdefender product**.
     f. Wait for the uninstall process to complete and then reboot your system.
3. Reinstall your Bitdefender product.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 201).

## 31.3. I can no longer use an application

This issue occurs when you are trying to use a program which was working normally before installing Bitdefender.

After installing Bitdefender you may encounter one of these situations:

- You could receive a message from Bitdefender that the program is trying to make a modification to the system.
- You could receive an error message from the program you're trying to use.

This type of situation occurs when the Active Virus Control module mistakenly detects some applications as malicious.

Active Virus Control is a Bitdefender module which constantly monitors the applications running on your system and reports those with potentially malicious behavior. Since this feature is based on a heuristic system, there may be cases when legitimate applications are reported by Active Virus Control.

When this situation occurs, you can exclude the respective application from being monitored by Active Virus Control.

To add the program to the exclusions list, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar..
3. In the **Settings Overview** window, select **Antivirus**.
4. In the **Antivirus Settings** window, select the **Exclusions** tab.
5. Click the **Excluded Processes** link. In the window that appears, you can manage the Active Virus Control process exclusions.
6. Add exclusions by following these steps:
   a. Click the **Add** button, located at the top of the exclusions table.
   b. Click **Browse**, find and select the application you want to be excluded and then click **OK**.
   c. Keep the **Allow** option selected to prevent Active Virus Control from blocking the application.
   d. Click **Add**.

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 201).

## 31.4. I cannot connect to the Internet

You may notice that a program or a web browser can no longer connect to the Internet or access network services after installing Bitdefender.

In this case, the best solution is to configure Bitdefender to automatically allow connections to and from the respective software application:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.

3. In the **Settings Overview** window, select **Firewall**.
4. In the **Firewall Settings** window, select the **Settings** tab.
5. Under Firewall Rules, click **Application Rules**.
6. To add an application rule, click the corresponding button.
7. Click **Browse** and select the application the rule applies to.
8. Select all the network types available.
9. Go to **Permission** and select **Allow**.

Close Bitdefender, open the software application and try again to connect to the Internet.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 201).

## 31.5. I cannot access a device on my network

Depending on the network you are connected to, the Bitdefender firewall may block the connection between your system and another device (such as another computer or a printer). As a result, you may no longer share or print files.

In this case, the best solution is to configure Bitdefender to automatically allow connections to and from the respective device. For each network connection you can configure a special trusted zone.

A trusted zone is a device that you fully trust. All traffic between your computer and the trusted device is allowed. To share resources with specific devices, such as computers or printers, add them as trusted zones.

To add a trusted zone on your network adapters, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar..
3. In the **Settings Overview** window, select **Firewall**.
4. In the **Firewall Settings** window, select the **Settings** tab.
5. Under Firewall Rules, click **Adapter Rules**.
6. To add a zone, click the corresponding button. A new window displaying the IP addresses of the devices connected to the network will appear.
7. Select the IP address of the computer or the printer you want to add, or type an address or address range in the provided text box.
8. Select **Allow** and then click **OK** and **Close**.

If you still cannot connect to the device, the issue may not be caused by Bitdefender.

Check for other potential causes, such as the following:

- The firewall on the other computer may block file and printer sharing with your computer.
  - If the Windows Firewall is used, it can be configured to allow file and printer sharing as follows:
    - In **Windows XP**:
      1. Click **Start**, go to **Control Panel** and select **Security Center**.
      2. Open the Windows Firewall settings window and select **Exceptions** tab.
      3. Select the **File and Printer Sharing** check box.
    - In **Windows Vista and Windows 7**:
      1. Click **Start**, go to **Control Panel** and select **System and Security**.
      2. Go to **Windows Firewall** and click **Allow a program through Windows Firewall**.
      3. Select **File and Printer Sharing** check box.
    - In **Windows 8**:
      1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
      2. Click **System and Security**, go to **Windows Firewall** and select **Allow an app through Windows Firewall**.
      3. Select **File and Printer Sharing** check box and click **OK**.
  - If another firewall program is used, please refer to its documentation or help file.
- General conditions that may prevent using or connecting to the shared printer:
  - You may need to log on to a Windows administrator account to access the shared printer.
  - Permissions are set for the shared printer to allow access to specific computer and users only. If you are sharing your printer, check the permissions set for the printer to see if the user on the other computer is allowed access to the printer. If you are trying to connect to a shared printer, check with the user on the other computer if you have permission to connect to the printer.
  - The printer connected to your computer or to the other computer is not shared.
  - The shared printer is not added on the computer.

Note

To learn how to manage printer sharing (share a printer, set or remove permissions for a printer, connect to a network printer or to a shared printer), go to the Windows Help and Support Center (in the Start menu, click **Help and Support**).

- Access to a network printer may be restricted to specific computers or users only. You should check with the network administrator if you have permission to connect to that printer.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 201).

## 31.6. My Internet is slow

This situation may appear after you install Bitdefender. The issue could be caused by errors in the Bitdefender firewall configuration.

To troubleshoot this situation, follow these steps:

1. Open the Bitdefender window.
2. On the **Firewall** panel, click the switch to turn off **Firewall**.
3. Check if your Internet connection improved with the Bitdefender firewall disabled.
   - If you still have a slow Internet connection, the issue may not be caused by Bitdefender. You should contact your Internet Service Provider to verify if the connection is operational on their side.

     If you receive confirmation from your Internet Service Provider that the connection is operational on their side and the issue still persists, contact Bitdefender as described in section "*Asking for help*" (p. 201).
   - If the Internet connection improved after disabling the Bitdefender firewall, follow these steps:
     a. Open the Bitdefender window.
     b. On the **Firewall** panel, click the switch to turn on **Firewall**.
     c. Click the **Settings** button on the upper toolbar..
     d. In the **Settings Overview** window, select **Firewall**.
     e. In the **Firewall Settings** window, select the **Advanced** tab.
     f. Go to **Internet connection sharing** and click the switch to turn it on.
     g. Go to **Block port scans** and click the switch to turn it off.
     h. Click to return to the main window.
     i. On the **Firewall** panel, click **Manage adapters**.
     j. Go to **Network Type** and select **Home/Office**.
     k. Go to **Stealth Mode** and set it to **Remote**. Set the **Generic** to **Yes**.
     l. Close Bitdefender, reboot the system and check the Internet connection speed.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 201).

## 31.7. How to update Bitdefender on a slow Internet connection

If you have a slow Internet connection (such as dial-up), errors may occur during the update process.

To keep your system up to date with the latest Bitdefender malware signatures, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Update**.
4. In the **Update Settings** window, select the **Update** tab.
5. Under **Update processing rules**, select **Prompt before downloading**.
6. Click to return to the main window.
7. Go to the **Update** panel and click **Update Now**.
8. Select only **Signatures updates** and then click **OK**.
9. Bitdefender will download and install only the malware signature updates.

## 31.8. My computer is not connected to the Internet. How do I update Bitdefender?

If your computer is not connected to the Internet, you must download the updates manually to a computer with Internet access and then transfer them to your computer using a removable device, such as a flash drive.

Follow these steps:

1. On a computer with Internet access, open a web browser and go to:

   http://www.bitdefender.com/site/view/Desktop-Products-Updates.html
2. In the **Manual Update** column, click the link corresponding to your product and system architecture. If you do not know whether your Windows is running on 32 or 64 bits, please refer to "*Am I using a 32 bit or a 64 bit version of Windows?*" (p. 71).
3. Save the file named `weekly.exe` to the system.
4. Transfer the downloaded file on a removable device, such as a flash drive, and then to your computer.
5. Double-click the file and follow the wizard steps.

## 31.9. Bitdefender services are not responding

This article helps you troubleshoot the **Bitdefender Services are not responding** error. You may encounter this error as follows:

- The Bitdefender icon in the system tray is grayed out and you are informed that the Bitdefender services are not responding.
- The Bitdefender window indicates that the Bitdefender services are not responding.

The error may be caused by one of the following conditions:

- temporary communication errors between the Bitdefender services.
- some of the Bitdefender services are stopped.
- other security solutions running on your computer at the same time with Bitdefender.

To troubleshoot this error, try these solutions:

1. Wait a few moments and see if anything changes. The error may be temporary.
2. Restart the computer and wait a few moments until Bitdefender is loaded. Open Bitdefender to see if the error persists. Restarting the computer usually solves the problem.
3. Check if you have any other security solution installed as they may disrupt the normal operation of Bitdefender. If this is the case, we recommend you to remove all of the other security solutions and then reinstall Bitdefender.

   For more information, please refer to "*How do I remove other security solutions?*" (p. 72).

If the error persists, please contact our support representatives for help as described in section "*Asking for help*" (p. 201).

## 31.10. Antispam filter does not work properly

This article helps you troubleshoot the following problems concerning the Bitdefender Antispam filtering operation:

- A number of legitimate e-mail messages are marked as `[spam]`.
- Many spam messages are not marked accordingly by the antispam filter.
- The antispam filter does not detect any spam message.

### 31.10.1. Legitimate messages are marked as [spam]

Legitimate messages are marked as `[spam]` simply because they look like spam to the Bitdefender antispam filter. You can normally solve this problem by adequately configuring the Antispam filter.

Bitdefender automatically adds the receivers of your e-mail messages to a Friends List. The e-mail messages received from the contacts in the Friends list are considered to be legitimate. They are not verified by the antispam filter and, thus, they are never marked as [spam].

The automatic configuration of the Friends list does not prevent the detection errors that may occur in these situations:

- You receive a lot of solicited commercial mail as a result of subscribing on various websites. In this case, the solution is to add the e-mail addresses from which you receive such e-mail messages to the Friends list.
- A significant part of your legitimate mail is from people to whom you never e-mailed before, such as customers, potential business partners and others. Other solutions are required in this case.

1. If you are using one of the mail clients Bitdefender integrates into, indicate detection errors.

   Note
   Bitdefender integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, please refer to "*Supported e-mail clients and protocols*" (p. 101).

2. Decrease antispam protection level. By decreasing the protection level, the antispam filter will need more spam indications to classify an e-mail message as spam. Try this solution only if many legitimate messages (including solicited commercial messages) are incorrectly detected as spam.

## Add contacts to Friends List

If you are using a supported mail client, you can easily add the senders of legitimate messages to the Friends list. Follow these steps:

1. In your mail client, select an e-mail message from the sender that you want to add to the Friends list.
2. Click the **Add Friend** button on the Bitdefender antispam toolbar.
3. You may be asked to acknowledge the addresses added to the Friends list. Select **Don't show this message again** and click **OK**.

You will always receive e-mail messages from this address no matter what they contain.

If you are using a different mail client, you can add contacts to the Friends list from the Bitdefender interface. Follow these steps:

1. Open the Bitdefender window.

2. On the **Antispam** panel, click **Manage** and select **Friends** from the drop-down menu.

   A configuration window will appear.

3. Type the e-mail address you always want to receive e-mail messages from and then click **Add**. You can add as many e-mail addresses as you want.

4. Click **OK** to save the changes and close the window.

### Indicate detection errors

If you are using a supported mail client, you can easily correct the antispam filter (by indicating which e-mail messages should not have been marked as `[spam]`). Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the junk mail folder where spam messages are moved.
3. Select the legitimate message incorrectly marked as `[spam]` by Bitdefender.
4. Click the **Add Friend** button on the Bitdefender antispam toolbar to add the sender to the Friends list. You may need to click **OK** to acknowledge. You will always receive e-mail messages from this address no matter what they contain.
5. Click the **Not Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). The e-mail message will be moved to the Inbox folder.

### Decrease antispam protection level

To decrease the antispam protection level, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antispam**.
4. In the **Antispam Settings** window, select the **Settings** tab.
5. Move the slider lower on the scale.

## 31.10.2. Many spam messages are not detected

If you are receiving many spam messages that are not marked as `[spam]`, you must configure the Bitdefender antispam filter so as to improve its efficiency.

Try the following solutions:

1. If you are using one of the mail clients Bitdefender integrates into, indicate undetected spam messages.

Note

Bitdefender integrates into the most commonly used mail clients through an easy-to-use antispam toolbar. For a complete list of supported mail clients, please refer to "*Supported e-mail clients and protocols*" (p. 101).

2. Add spammers to the Spammers list. The e-mail messages received from addresses in the Spammers list are automatically marked as [spam].
3. Increase antispam protection level. By increasing the protection level, the antispam filter will need less spam indications to classify an e-mail message as spam.

## Indicate undetected spam messages

If you are using a supported mail client, you can easily indicate which e-mail messages should have been detected as spam. Doing so helps improve the efficiency of the antispam filter. Follow these steps:

1. Open your mail client.
2. Go to the Inbox folder.
3. Select the undetected spam messages.
4. Click the **Is Spam** button on the Bitdefender antispam toolbar (normally located in the upper part of the mail client window). They are immediately marked as [spam] and moved to the junk mail folder.

## Add spammers to Spammers List

If you are using a supported mail client, you can easily add the senders of the spam messages to the Spammers list. Follow these steps:

1. Open your mail client.
2. Go to the junk mail folder where spam messages are moved.
3. Select the messages marked as [spam] by Bitdefender.
4. Click the **Add Spammer** button on the Bitdefender antispam toolbar.
5. You may be asked to acknowledge the addresses added to the Spammers list. Select **Don't show this message again** and click **OK**.

If you are using a different mail client, you can manually add spammers to the Spammers list from the Bitdefender interface. It is convenient to do this only when you have received several spam messages from the same e-mail address. Follow these steps:

1. Open the Bitdefender window.

2. On the **Antispam** panel, click **Manage** and select **Spammers** from the drop-down menu.

   A configuration window will appear.

3. Type the spammer's e-mail address and then click the **Add**. You can add as many e-mail addresses as you want.

4. Click **OK** to save the changes and close the window.

### Increase antispam protection level

To increase the antispam protection level, follow these steps:

1. Open the Bitdefender window.
2. Click the **Settings** button on the upper toolbar.
3. In the **Settings Overview** window, select **Antispam**.
4. In the **Antispam Settings** window, select the **Settings** tab.
5. Move the slider higher on the scale.

## 31.10.3. Antispam filter does not detect any spam message

If no spam message is marked as `[spam]`, there may be a problem with the Bitdefender Antispam filter. Before troubleshooting this problem, make sure it is not caused by one of the following conditions:

- Antispam protection might be turned off. To verify the antispam protection status, open the Bitdefender window and check the switch in the **Antispam** panel.

  If Antispam is turned off, this is what is causing your problem. Click the switch to turn on your antispam protection.

- The Bitdefender Antispam protection is available only for e-mail clients configured to receive e-mail messages via the POP3 protocol. This means the following:

  - E-mail messages received via web-based e-mail services (such as Yahoo, Gmail, Hotmail or other) are not filtered for spam by Bitdefender.
  - If your e-mail client is configured to receive e-mail messages using other protocol than POP3 (for example, IMAP4), the Bitdefender Antispam filter does not check them for spam.

  **Note**

  POP3 is one of the most widely used protocols for downloading e-mail messages from a mail server. If you do not know the protocol that your e-mail client uses to download e-mail messages, ask the person who configured your e-mail client.

- Bitdefender Total Security doesn't scan Lotus Notes POP3 traffic.

A possible solution is to repair or reinstall the product. However, you may want to contact Bitdefender for support instead, as described in section "*Asking for help*" (p. 201).

## 31.11. The Autofill feature in my Wallet doesn't work

You have saved your online credentials in your Bitdefender Wallet and you noticed that the autofill is not working. Usually, this issue appears when the Bitdefender Wallet extension is not installed in your browser.

To fix this situation, follow these steps:

- In **Internet Explorer:**
  1. Open Internet Explorer.
  2. Click Tools.
  3. Click Manage Add-ons.
  4. Click Toolbars and Extensions.
  5. Point **Bitdefender Wallet** and click Enable.
- In **Mozilla Firefox:**
  1. Open Mozilla Firefox.
  2. Click Tools.
  3. Click Add-ons.
  4. Click Extensions.
  5. Point **Bitdefender Wallet** and click Enable.
- In **Google Chrome:**
  1. Open Google Chrome.
  2. Go to the Menu icon.
  3. Click Settings.
  4. Click Extensions.
  5. Point **Bitdefender Wallet** and click Enable.

Note
The add-on will be enabled after you restart your web browser.

Now check if the autofill feature in Wallet works for your online accounts.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 201).

## 31.12. Bitdefender removal failed

If you want to remove your Bitdefender product and you notice that the process hangs out or the system freezes, click **Cancel** to abort the action. If this does not work, restart the system.

When removal fails, some Bitdefender registry keys and files may remain in your system. Such remainders may prevent a new installation of Bitdefender. They may also affect system performance and stability.

In order to completely remove Bitdefender from your system, follow these steps:

- In **Windows XP**:
  1. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.
  2. Wait a few moments until the list of installed software is displayed.
  3. Find **Bitdefender** and select **Remove**.
  4. Click **Remove** and then **FULL uninstall of Bitdefender**.
  5. You have the following options:
     - **Uninstall and stay protected** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will be installed on your system to protect you against malware.
     - **Uninstall without the app** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will not be installed.

     Select the desired option and click **Next**.
  6. Wait for the uninstall process to complete and then reboot your system.
- In **Windows Vista** and **Windows 7**:
  1. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.
  2. Wait a few moments until the installed software list is displayed.
  3. Find **Bitdefender** and select **Uninstall**.
  4. Click **Remove** and then **FULL uninstall of Bitdefender**.
  5. You have the following options:
     - **Uninstall and stay protected** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will be installed on your system to protect you against malware.
     - **Uninstall without the app** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will not be installed.

     Select the desired option and click **Next**.
  6. Wait for the uninstall process to complete and then reboot your system.

- In **Windows 8**:

  1. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.
  2. Click **Uninstall a program** or **Programs and Features**.
  3. Wait a few moments until the installed software list is displayed.
  4. Find **Bitdefender** and select **Uninstall**.
  5. Click **Remove** and then **FULL uninstall of Bitdefender**.
  6. You have the following options:

     - **Uninstall and stay protected** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will be installed on your system to protect you against malware.
     - **Uninstall without the app** - will completely remove Bitdefender. Bitdefender 60-Second Virus Scanner will not be installed.

     Select the desired option and click **Next**.
  7. Wait for the uninstall process to complete and then reboot your system.

Note

Bitdefender 60-Second Virus Scanner is a free application which uses in-the-cloud scanning technology to detect malicious programs and threats in less than 60 seconds.

## 31.13. My system doesn't boot up after installing Bitdefender

If you just installed Bitdefender and cannot reboot your system in normal mode anymore there may be various reasons for this issue.

Most probably this is caused by a previous Bitdefender installation which was not removed properly or by another security solution still present on the system.

This is how you may address each situation:

- **You had Bitdefender before and you did not remove it properly.**

  To solve this, follow these steps:

  1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to *"How do I restart in Safe Mode?"* (p. 74).
  2. Remove Bitdefender from your system:

     - In **Windows XP**:

       a. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.

       b. Wait a few moments until the list of installed software is displayed.

c. Find **Bitdefender** and select **Remove**.

d. Click **Remove** and then **Reinstall/change my Bitdefender product**.

e. Wait for the uninstall process to complete.

f. Reboot your system in normal mode.

▶ In **Windows Vista** and **Windows 7**:

a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.

b. Wait a few moments until the installed software list is displayed.

c. Find **Bitdefender** and select **Uninstall**.

d. Click **Remove** and then **Reinstall/change my Bitdefender product**.

e. Wait for the uninstall process to complete.

f. Reboot your system in normal mode.

▶ In **Windows 8**:

a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.

b. Click **Uninstall a program** or **Programs and Features**.

c. Wait a few moments until the installed software list is displayed.

d. Find **Bitdefender** and select **Uninstall**.

e. Click **Remove** and then **Reinstall/change my Bitdefender product**.

f. Wait for the uninstall process to complete.

g. Reboot your system in normal mode.

3. Reinstall your Bitdefender product.

● **You had a different security solution before and you did not remove it properly.**

To solve this, follow these steps:

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to "*How do I restart in Safe Mode?*" (p. 74).
2. Remove Bitdefender from your system:

▶ In **Windows XP**:

a. Click **Start**, go to **Control Panel** and double-click **Add / Remove programs**.

b. Wait a few moments until the list of installed software is displayed.

c. Find **Bitdefender** and select **Remove**.

d. Click **Remove** and then **Reinstall/change my Bitdefender product**.

e. Wait for the uninstall process to complete and then reboot your system.

- In **Windows Vista** and **Windows 7**:

  a. Click **Start**, go to **Control Panel** and double-click **Programs and Features**.

  b. Wait a few moments until the installed software list is displayed.

  c. Find **Bitdefender** and select **Uninstall**.

  d. Click **Remove** and then **Reinstall/change my Bitdefender product**.

  e. Wait for the uninstall process to complete and then reboot your system.

- In **Windows 8**:

  a. From the Windows Start screen, locate **Control Panel** (for example, you can start typing "Control Panel" directly in the Start screen) and then click its icon.

  b. Click **Uninstall a program** or **Programs and Features**.

  c. Wait a few moments until the installed software list is displayed.

  d. Find **Bitdefender** and select **Uninstall**.

  e. Click **Remove** and then **Reinstall/change my Bitdefender product**.

  f. Wait for the uninstall process to complete and then reboot your system.

3. In order to correctly uninstall the other software, go to their website and run their uninstall tool or contact them directly in order to provide you with the uninstall guidelines.
4. Reboot your system in normal mode and reinstall Bitdefender.

**You have already followed the steps above and the situation is not solved.**

To solve this, follow these steps:

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to “*How do I restart in Safe Mode?*” (p. 74).
2. Use the System Restore option from Windows to restore the computer to an earlier date before installing the Bitdefender product. To find out how to do this, please refer to “*How do I use System Restore in Windows?*” (p. 73).
3. Reboot the system in normal mode and contact our support representatives for help as described in section “*Asking for help*” (p. 201).

# 32. Removing malware from your system

Malware can affect your system in many different ways and the Bitdefender approach depends on the type of malware attack. Because viruses change their behavior frequently, it is difficult to establish a pattern for their behavior and their actions.

There are situations when Bitdefender cannot automatically remove the malware infection from your system. In such cases, your intervention is required.


- "*Bitdefender Rescue Mode*" (p. 192)
- "*What to do when Bitdefender finds viruses on your computer?*" (p. 194)
- "*How do I clean a virus in an archive?*" (p. 195)
- "*How do I clean a virus in an e-mail archive? *" (p. 196)
- "*What to do if I suspect a file as being dangerous?*" (p. 197)
- "*How to clean the infected files from System Volume Information*" (p. 197)
- "*What are the password-protected files in the scan log?*" (p. 198)
- "*What are the skipped items in the scan log?*" (p. 199)
- "*What are the over-compressed files in the scan log?*" (p. 199)
- "*Why did Bitdefender automatically delete an infected file?*" (p. 199)


If you cannot find your problem here, or if the presented solutions do not solve it, you can contact the Bitdefender technical support representatives as presented in chapter "*Asking for help*" (p. 201).

## 32.1. Bitdefender Rescue Mode

**Rescue Mode** is a Bitdefender feature that allows you to scan and disinfect all existing hard drive partitions outside of your operating system.

Once Bitdefender Total Security is installed, Rescue Mode can be used even if you are no longer able to boot into Windows.

### Starting your system in Rescue Mode

You can enter Rescue Mode in one of two ways:

From the Bitdefender window

To enter Rescue Mode directly from Bitdefender, follow these steps:

1. Open the Bitdefender window.
2. On the **Antivirus** panel, click **Scan Now** and select **Rescue Mode** from the drop-down menu.

   A confirmation window will appear. Click **Yes** to reboot your computer.

3. After the computer restarts, a menu will appear prompting you to select an operating system. Choose **Bitdefender Rescue Image** and press the **Enter** key to boot into a Bitdefender environment from where you can clean up your Windows partition.
4. If prompted, press **Enter** and select the screen resolution closest to the one you normally use. Then press **Enter** again.

   Bitdefender Rescue Mode will load in a few moments.

Boot your computer directly into Rescue Mode

If Windows no longer starts, you can boot your computer directly into Bitdefender Rescue Mode by following the steps below:

Note

This method is not available on computers running Windows XP.

1. Start / reboot your computer and start pressing the **space** key on your keyboard before the Windows logo appears.
2. A menu will appear prompting you to select an operating system to start. Press **TAB** to go to the tools area. Choose **Bitdefender Rescue Image** and press the **Enter** key to boot into a Bitdefender environment from where you can clean up your Windows partition.
3. If prompted, press **Enter** and select the screen resolution closest to the one you normally use. Then press **Enter** again.

   Bitdefender Rescue Mode will load in a few moments.

## Scanning your system in Rescue Mode

To scan your system in Rescue Mode, follow these steps:

1. Enter Rescue Mode, as described in “Starting your system in Rescue Mode” (p. 192).
2. The Bitdefender logo will appear and the antivirus engines will start to be copied.
3. A welcome window will then appear. Click **Continue**.
4. An update of the antivirus signatures is started.
5. After the update is completed, the Bitdefender On-demand Antivirus Scanner window will appear.
6. Click **Scan Now**, select the scan target in the window that appears and click **Open** to start scanning.

   It is recommended to scan your entire Windows partition.

Note
When working in Rescue Mode, you are dealing with Linux-type partition names. Disk partitions will appear as `sda1` probably corresponding to the `(C:)` Windows-type partition, `sda2` corresponding to `(D:)` and so on.

7. Wait for the scan to complete. If any malware is detected, follow the instructions to remove the threat.
8. To exit Rescue Mode, right-click in an empty area of the desktop, select **Exit** in the menu that appears and then choose whether to reboot or shut down the computer.

## 32.2. What to do when Bitdefender finds viruses on your computer?

You may find out there is a virus on your computer in one of these ways:

- You scanned your computer and Bitdefender found infected items on it.
- A virus alert informs you that Bitdefender blocked one or multiple viruses on your computer.

In such situations, update Bitdefender to make sure you have the latest malware signatures and run a System Scan to analyze the system.

As soon as the system scan is over, select the desired action for the infected items (Disinfect, Delete, Move to quarantine).

Warning
If you suspect the file is part of the Windows operating system or that it is not an infected file, do not follow these steps and contact Bitdefender Customer Care as soon as possible.

If the selected action could not be taken and the scan log reveals an infection which could not be deleted, you have to remove the file(s) manually:

**The first method can be used in normal mode**:

1. Turn off the Bitdefender real-time antivirus protection:
   a. Open the Bitdefender window.
   b. Click the **Settings** button in the upper toolbar.
   c. In the **Settings Overview** window, select **Antivirus**.
   d. Click the **Shield** tab in the **Antivirus Settings** window.
   e. Click the switch to turn off **On-access scanning**.
2. Display hidden objects in Windows. To find out how to do this, please refer to "*How do I display hidden objects in Windows?*" (p. 72).

3. Browse to the location of the infected file (check the scan log) and delete it.
4. Turn on the Bitdefender real-time antivirus protection.

**In case the first method failed to remove the infection, follow these steps**:

1. Reboot your system and enter in Safe Mode. To find out how to do this, please refer to "*How do I restart in Safe Mode?*" (p. 74).
2. Display hidden objects in Windows. To find out how to do this, please refer to "*How do I display hidden objects in Windows?*" (p. 72).
3. Browse to the location of the infected file (check the scan log) and delete it.
4. Reboot your system and enter in normal mode.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 201).

## 32.3. How do I clean a virus in an archive?

An archive is a file or a collection of files compressed under a special format to reduce the space on disk necessary for storing the files.

Some of these formats are open formats, thus providing Bitdefender the option to scan inside them and then take appropriate actions to remove them.

Other archive formats are partially or fully closed, and Bitdefender can only detect the presence of viruses inside them, but is not able to take any other actions.

If Bitdefender notifies you that a virus has been detected inside an archive and no action is available, it means that removing the virus is not possible due to restrictions on the archive's permission settings.

Here is how you can clean a virus stored in an archive:

1. Identify the archive that includes the virus by performing a System Scan of the system.
2. Turn off the Bitdefender real-time antivirus protection:
   a. Open the Bitdefender window.
   b. Click the **Settings** button in the upper toolbar.
   c. In the **Settings Overview** window, select **Antivirus**.
   d. Click the **Shield** tab in the **Antivirus Settings** window.
   e. Click the switch to turn off **On-access scanning**.
3. Go to the location of the archive and decompress it using an archiving application, like WinZip.
4. Identify the infected file and delete it.
5. Delete the original archive in order to make sure the infection is totally removed.

6. Recompress the files in a new archive using an archiving application, like WinZip.
7. Turn on the Bitdefender real-time antivirus protection and run a Full system scan in order to make sure there is no other infection on the system.

Note
It's important to note that a virus stored in an archive is not an immediate threat to your system, since the virus has to be decompressed and executed in order to infect your system.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 201).

## 32.4. How do I clean a virus in an e-mail archive?

Bitdefender can also identify viruses in e-mail databases and e-mail archives stored on disk.

Sometimes it is necessary to identify the infected message using the information provided in the scan report, and delete it manually.

Here is how you can clean a virus stored in an e-mail archive:

1. Scan the e-mail database with Bitdefender.
2. Turn off the Bitdefender real-time antivirus protection:
   a. Open the Bitdefender window.
   b. Click the **Settings** button in the upper toolbar.
   c. In the **Settings Overview** window, select **Antivirus**.
   d. Click the **Shield** tab in the **Antivirus Settings** window.
   e. Click the switch to turn off **On-access scanning**.
3. Open the scan report and use the identification information (Subject, From, To) of the infected messages to locate them in the e-mail client.
4. Delete the infected messages. Most e-mail clients also move the deleted message to a recovery folder, from which it can be recovered. You should make sure the message is deleted also from this recovery folder.
5. Compact the folder storing the infected message.
   - In Outlook Express: On the File menu, click Folder, then Compact All Folders.
   - In Microsoft Outlook 2007: On the File menu, click Data File Management. Select the personal folders (.pst) files you intend to compact, and click Settings. Click Compact Now.
   - In Microsoft Outlook 2010 / 2013: On the File menu, click Info and then Account settings (Add and remove accounts or change existing connection settings).

Then click Data File, select the personal folders (.pst) files you intend to compact, and click Settings. Click Compact Now.

6. Turn on the Bitdefender real-time antivirus protection.

If this information was not helpful, you can contact Bitdefender for support as described in section "*Asking for help*" (p. 201).

## 32.5. What to do if I suspect a file as being dangerous?

You may suspect a file from your system as being dangerous, even though your Bitdefender product did not detect it.

To make sure your system is protected, follow these steps:

1. Run a **System Scan** with Bitdefender. To find out how to do this, please refer to "*How do I scan my system?*" (p. 51).
2. If the scan result appears to be clean, but you still have doubts and want to make sure about the file, contact our support representatives so that we may help you.

   To find out how to do this, please refer to "*Asking for help*" (p. 201).

## 32.6. How to clean the infected files from System Volume Information

The System Volume Information folder is a zone on your hard drive created by the Operating System and used by Windows for storing critical information related to the system configuration.

The Bitdefender engines can detect any infected files stored by the System Volume Information, but being a protected area it may not be able to remove them.

The infected files detected in the System Restore folders will appear in the scan log as follows:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

To completely and immediately remove the infected file or files in the data store, disable and re-enable the System Restore feature.

When System Restore is turned off, all the restore points are removed.

When System Restore is turned on again, new restore points are created as the schedule and events require.

In order to disable the System Restore follow these steps:

- **For Windows XP:**
  1. Follow this path: **Start → All Programs → Accessories → System Tool → System Restore**
  2. Click **System Restore Settings** located on the left hand side of the window.

3. Select the **Turn off System Restore** check box on all drives, and click **Apply**.
4. When you are warned that all existing Restore Points will be deleted, click **Yes** to continue.
5. To turn on the System Restore, clear the **Turn off System Restore** check box on all drives, and click **Apply**.

- **For Windows Vista:**
  1. Follow this path: **Start** → **Control Panel** → **System and Maintenance** → **System**
  2. In the left pane, click **System Protection**.

     If you are prompted for an administrator password or confirmation, type the password or provide confirmation.
  3. To turn off the System Restore clear the check boxes corresponding to each drive and click **OK**.
  4. To turn on the System Restore select the check boxes corresponding to each drive and click **OK**.
- **For Windows 7:**
  1. Click **Start**, right-click **Computer** and click **Properties**.
  2. Click **System protection** link in the left pane.
  3. In the **System protection** options, select each drive letter and click **Configure**.
  4. Select **Turn off system protection** and click **Apply**.
  5. Click **Delete**, click **Continue** when prompted and then click **OK**.
- **For Windows 8:**
  1. From the Windows Start screen, locate **Computer** (for example, you can start typing "Computer" directly in the Start screen) and then click its icon.
  2. Click **System protection** link in the left pane.
  3. In the **System protection** options, select each drive letter and click **Configure**.
  4. Select **Turn off system protection** and click **Apply**.

If this information was not helpful, you can contact Bitdefender for support as described in section *"Asking for help"* (p. 201).

## 32.7. What are the password-protected files in the scan log?

This is only a notification which indicates that Bitdefender has detected these files are either protected with a password or by some form of encryption.

Most commonly, the password-protected items are:

- Files that belong to another security solution.
- Files that belong to the operating system.

In order to actually scan the contents, these files would need to either be extracted or otherwise decrypted.

Should those contents be extracted, Bitdefender's real-time scanner would automatically scan them to keep your computer protected. If you want to scan those files with Bitdefender, you have to contact the product manufacturer in order to provide you with more details on those files.

Our recommendation to you is to ignore those files because they are not a threat for your system.

## 32.8. What are the skipped items in the scan log?

All files that appear as Skipped in the scan report are clean.

For increased performance, Bitdefender does not scan files that have not changed since the last scan.

## 32.9. What are the over-compressed files in the scan log?

The over-compressed items are elements which could not be extracted by the scanning engine or elements for which the decryption time would have taken too long making the system unstable.

Overcompressed means that Bitdefender skipped scanning within that archive because unpacking it proved to take up too many system resources. The content will be scanned on real time access if needed.

## 32.10. Why did Bitdefender automatically delete an infected file?

If an infected file is detected, Bitdefender will automatically attempt to disinfect it. If disinfection fails, the file is moved to quarantine in order to contain the infection.

For particular types of malware, disinfection is not possible because the detected file is entirely malicious. In such cases, the infected file is deleted from the disk.

This is usually the case with installation files that are downloaded from untrustworthy websites. If you find yourself in such a situation, download the installation file from the manufacturer's website or other trusted website.

# Contact us

# 33. Asking for help

Bitdefender provides its customers with an unparalleled level of fast and accurate support. If you experience any issue or if you have any question about your Bitdefender product, you can use several online resources to find a solution or an answer. At the same time, you can contact the Bitdefender Customer Care team. Our support representatives will answer your questions in a timely manner and will provide you with the assistance you need.

The "*Solving common issues*" (p. 173) section provides the necessary information regarding the most frequent issues you may encounter when using this product.

If you do not find an answer to your question in the provided resources, you can contact us directly:

- "Contact us directly from your Bitdefender product" (p. 201)
- "Contact us through our online Support Center" (p. 202)

Important
To contact the Bitdefender Customer Care you must register your Bitdefender product. For more information, please refer to "*Registering Bitdefender*" (p. 33).

## Contact us directly from your Bitdefender product

If you have a working Internet connection, you can contact Bitdefender for assistance directly from the product interface.

Follow these steps:

1. Open the Bitdefender window.
2. Click the **Help and Support** link, located at the bottom-right corner of the window.
3. You have the following options:
   - **Bitdefender Help**.

     Browse the Bitdefender documentation articles and try the proposed solutions.
   - **Support Center**

     Access our database and search for the necessary information.
   - **Contact Support**

     Use the **Contact Support** button to launch the Support Tool and contact the Customer Care Department. You can navigate through the wizard using the **Next** button. To exit the wizard, click **Cancel**.

     a. Select the agreement check box and click **Next**.

     b. Complete the submission form with the necessary data:

i. Enter your e-mail address.

ii. Enter your full name.

iii. Choose your country from the corresponding menu.

iv. Enter a description of the issue you encountered.

c. Please wait for a few minutes while Bitdefender gathers product related information. This information will help our engineers find a solution to your problem.

d. Click **Finish** to send the information to the Bitdefender Customer Care Department. You will be contacted as soon as possible.

## Contact us through our online Support Center

If you cannot access the necessary information using the Bitdefender product, please refer to our online Support Center:

1. Go to http://www.bitdefender.com/support/consumer.html. The Bitdefender Support Center hosts numerous articles that contain solutions to Bitdefender-related issues.
2. Use the search bar at the top of the window to find articles that may provide a solution to your problem. To search, just type a term in the Search bar and click **Search**.
3. Read the relevant articles or documents and try the proposed solutions.
4. If the solution does not solve your problem, go to http://www.bitdefender.com/support/contact-us.html and contact our support representatives.

# 34. Online resources

Several online resources are available to help you solve your Bitdefender-related problems and questions.

- Bitdefender Support Center: http://www.bitdefender.com/support/consumer.html
- Bitdefender Support Forum: http://forum.bitdefender.com
- the HOTforSecurity computer security portal: http://www.hotforsecurity.com

You can also use your favorite search engine to find out more information about computer security, the Bitdefender products and the company.

## 34.1. Bitdefender Support Center

The Bitdefender Support Center is an online repository of information about the Bitdefender products. It stores, in an easily accessible format, reports on the results of the ongoing technical support and bugfixing activities of the Bitdefender support and development teams, along with more general articles about virus prevention, the management of Bitdefender solutions with detailed explanations, and many other articles.

The Bitdefender Support Center is open to the public and freely searchable. The extensive information it contains is yet another means of providing Bitdefender customers with the technical knowledge and insight they need. All valid requests for information or bug reports coming from Bitdefender clients eventually find their way into the Bitdefender Support Center, as bugfix reports, workaround cheatsheets or informational articles to supplement product helpfiles.

The Bitdefender Support Center is available any time at http://www.bitdefender.com/support/consumer.html.

## 34.2. Bitdefender Support Forum

The Bitdefender Support Forum provides Bitdefender users with an easy way to get help and to help others.

If your Bitdefender product does not operate well, if it cannot remove specific viruses from your computer or if you have questions about the way it works, post your problem or question on the forum.

Bitdefender support technicians monitor the forum for new posts in order to assist you. You may also get an answer or a solution from a more experienced Bitdefender user.

Before posting your problem or question, please search the forum for a similar or related topic.

The Bitdefender Support Forum is available at http://forum.bitdefender.com, in 5 different languages: English, German, French, Spanish and Romanian. Click the **Home & Home Office Protection** link to access the section dedicated to consumer products.

## 34.3. HOTforSecurity Portal

HOTforSecurity is a rich source of computer security information. Here you can learn about the various threats your computer is exposed to when connected to the Internet (malware, phishing, spam, cyber-criminals).

New articles are posted regularly to keep you up-to-date with the latest threats discovered, the current security trends and other information on the computer security industry.

The HOTforSecurity web page is http://www.hotforsecurity.com.

# 35. Contact information

Efficient communication is the key to a successful business. During the past 10 years BITDEFENDER has established an unquestionable reputation by constantly striving for better communication so as to exceed the expectations of our clients and partners. Should you have any questions, do not hesitate to contact us.

## 35.1. Web addresses

Sales department: sales@bitdefender.com
Support Center: http://www.bitdefender.com/support/consumer.html
Documentation: documentation@bitdefender.com
Local distributors: http://www.bitdefender.com/partners
Partner program: partners@bitdefender.com
Media relations: pr@bitdefender.com
Careers: jobs@bitdefender.com
Virus submissions: virus_submission@bitdefender.com
Spam submissions: spam_submission@bitdefender.com
Report abuse: abuse@bitdefender.com
Web site: http://www.bitdefender.com

## 35.2. Local distributors

The Bitdefender local distributors are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters.

To find a Bitdefender distributor in your country:

1. Go to http://www.bitdefender.com/partners/#Partner Locator/.
2. Click the **Partner Locator** tab.
3. The contact information of the Bitdefender local distributors should be displayed automatically. If this does not happen, select the country you reside in to view the information.
4. If you do not find a Bitdefender distributor in your country, feel free to contact us by e-mail at sales@bitdefender.com. Please write your e-mail in English in order for us to be able to assist you promptly.

## 35.3. Bitdefender offices

The Bitdefender offices are ready to respond to any inquiries regarding their areas of operation, both in commercial and in general matters. Their respective addresses and contacts are listed below.

## U.S.A

**Bitdefender, LLC**
PO Box 667588
Pompano Beach, Fl 33066
Phone (office&sales): 1-954-776-6262
Sales: sales@bitdefender.com
Technical support: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.com

## UK and Ireland

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
E-mail: info@bitdefender.co.uk
Phone: +44 (0) 8451-305096
Sales: sales@bitdefender.co.uk
Technical support: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.co.uk

## Germany

**Bitdefender GmbH**
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Deutschland
Office: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Sales: vertrieb@bitdefender.de
Technical support: http://www.bitdefender.de/support/consumer.html
Web: http://www.bitdefender.de

## Spain

**Bitdefender España, S.L.U.**
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Phone: +34 902 19 07 65
Sales: comercial@bitdefender.es
Technical support: http://www.bitdefender.es/support/consumer.html
Website: http://www.bitdefender.es

## Romania

**BITDEFENDER SRL**
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Sales phone: +40 21 2063470
Sales e-mail: sales@bitdefender.ro
Technical support: http://www.bitdefender.ro/support/consumer.html
Website: http://www.bitdefender.ro

## United Arab Emirates

**Dubai Internet City**
Building 17, Office # 160
Dubai, UAE
Sales phone: 00971-4-4588935 / 00971-4-4589186
Sales e-mail: sales@bitdefender.com
Technical support: http://www.bitdefender.com/support/consumer.html
Website: http://www.bitdefender.com/world

# Glossary

**ActiveX**

ActiveX is a model for writing programs so that other programs and the operating system can call them. ActiveX technology is used with Microsoft Internet Explorer to make interactive Web pages that look and behave like computer programs, rather than static pages. With ActiveX, users can ask or answer questions, use push buttons, and interact in other ways with the Web page. ActiveX controls are often written using Visual Basic.

Active X is notable for a complete lack of security controls; computer security experts discourage its use over the Internet.

**Adware**

Adware is often combined with a host application that is provided at no charge as long as the user agrees to accept the adware. Because adware applications are usually installed after the user has agreed to a licensing agreement that states the purpose of the application, no offense is committed.

However, pop-up advertisements can become an annoyance, and in some cases degrade system performance. Also, the information that some of these applications collect may cause privacy concerns for users who were not fully aware of the terms in the license agreement.

**Archive**

A disk, tape, or directory that contains files that have been backed up.

A file that contains one or more files in a compressed format.

**Backdoor**

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers.

**Boot sector**

A sector at the beginning of each disk that identifies the disk's architecture (sector size, cluster size, and so on). For startup disks, the boot sector also contains a program that loads the operating system.

**Boot virus**

A virus that infects the boot sector of a fixed or floppy disk. An attempt to boot from a diskette infected with a boot sector virus will cause the virus to become active in memory. Every time you boot your system from that point on, you will have the virus active in memory.

**Browser**

Short for Web browser, a software application used to locate and display Web pages. Popular browsers include Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. These are graphical browsers, which means that they can display graphics as well as text. In addition, most modern browsers can present multimedia information, including sound and video, though they require plug-ins for some formats.

**Command line**

In a command line interface, the user types commands in the space provided directly on the screen using command language.

**Cookie**

Within the Internet industry, cookies are described as small files containing information about individual computers that can be analyzed and used by advertisers to track your online interests and tastes. In this realm, cookie technology is still being developed and the intention is to target ads directly to what you've said your interests are. It's a double-edge sword for many people because on one hand, it's efficient and pertinent as you only see ads about what you're interested in. On the other hand, it involves actually "tracking" and "following" where you go and what you click. Understandably so, there is a debate over privacy and many people feel offended by the notion that they are viewed as a "SKU number" (you know, the bar code on the back of packages that gets scanned at the grocery check-out line). While this viewpoint may be extreme, in some cases it is accurate.

**Disk drive**

It's a machine that reads data from and writes data onto a disk.

A hard disk drive reads and writes hard disks.

A floppy drive accesses floppy disks.

Disk drives can be either internal (housed within a computer) or external (housed in a separate box that connects to the computer).

**Download**

To copy data (usually an entire file) from a main source to a peripheral device. The term is often used to describe the process of copying a file from an online service to one's own computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

**E-mail**

Electronic mail. A service that sends messages on computers via local or global networks.

**Events**
An action or occurrence detected by a program. Events can be user actions, such as clicking a mouse button or pressing a key, or system occurrences, such as running out of memory.

**False positive**
Occurs when a scanner identifies a file as infected when in fact it is not.

**Filename extension**
The portion of a filename, following the final point, which indicates the kind of data stored in the file.

Many operating systems use filename extensions, e.g. Unix, VMS, and MS-DOS. They are usually from one to three letters (some sad old OSes support no more than three). Examples include "c" for C source code, "ps" for PostScript, "txt" for arbitrary text.

**Heuristic**
A rule-based method of identifying new viruses. This method of scanning does not rely on specific virus signatures. The advantage of the heuristic scan is that it is not fooled by a new variant of an existing virus. However, it might occasionally report suspicious code in normal programs, generating the so-called "false positive".

**IP**
Internet Protocol - A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets.

**Java applet**
A Java program which is designed to run only on a web page. To use an applet on a web page, you would specify the name of the applet and the size (length and width, in pixels) that the applet can utilize. When the web page is accessed, the browser downloads the applet from a server and runs it on the user's machine (the client). Applets differ from applications in that they are governed by a strict security protocol.

For example, even though applets run on the client, they cannot read or write data onto the client's machine. Additionally, applets are further restricted so that they can only read and write data from the same domain that they are served from.

**Keylogger**
A keylogger is an application that logs anything you type.

Keyloggers are not malicious in nature. They can be used for legitimate purposes, such as monitoring employees or children activity. However, they

are increasingly being used by cyber-criminals for malicious purposes (for example, to collect private data, such as login credentials and social security numbers).

**Macro virus**

A type of computer virus that is encoded as a macro embedded in a document. Many applications, such as Microsoft Word and Excel, support powerful macro languages.

These applications allow you to embed a macro in a document, and have the macro execute each time the document is opened.

**Mail client**

An e-mail client is an application that enables you to send and receive e-mail.

**Memory**

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips, and the word storage is used for memory that exists on tapes or disks. Every computer comes with a certain amount of physical memory, usually referred to as main memory or RAM.

**Non-heuristic**

This method of scanning relies on specific virus signatures. The advantage of the non-heuristic scan is that it is not fooled by what might seem to be a virus, and does not generate false alarms.

**Packed programs**

A file in a compression format. Many operating systems and applications contain commands that enable you to pack a file so that it takes up less memory. For example, suppose you have a text file containing ten consecutive space characters. Normally, this would require ten bytes of storage.

However, a program that packs files would replace the space characters by a special space-series character followed by the number of spaces being replaced. In this case, the ten spaces would require only two bytes. This is just one packing technique - there are many more.

**Path**

The exact directions to a file on a computer. These directions are usually described by means of the hierarchical filing system from the top down.

The route between any two points, such as the communications channel between two computers.

**Phishing**

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private

information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

**Polymorphic virus**

A virus that changes its form with each file it infects. Since they have no consistent binary pattern, such viruses are hard to identify.

**Port**

An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. Externally, personal computers have ports for connecting modems, printers, mice, and other peripheral devices.

In TCP/IP and UDP networks, an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic.

**Report file**

A file that lists actions that have occurred. Bitdefender maintains a report file listing the path scanned, the folders, the number of archives and files scanned, how many infected and suspicious files were found.

**Rootkit**

A rootkit is a set of software tools which offer administrator-level access to a system. The term was first used for the UNIX operating systems and it referred to recompiled tools which provided intruders administrative rights, allowing them to conceal their presence so as not to be seen by the system administrators.

The main role of rootkits is to hide processes, files, logins and logs. They may also intercept data from terminals, network connections or peripherals, if they incorporate the appropriate software.

Rootkits are not malicious in nature. For example, systems and even some applications hide critical files using rootkits. However, they are mostly used to hide malware or to conceal the presence of an intruder into the system. When combined with malware, rootkits pose a great threat to the integrity and the security of a system. They can monitor traffic, create backdoors into the system, alter files and logs and avoid detection.

**Script**

Another term for macro or batch file, a script is a list of commands that can be executed without user interaction.

**Spam**

Electronic junk mail or junk newsgroup postings. Generally known as any unsolicited e-mail.

**Spyware**

Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware's similarity to a Trojan horse is the fact that users unwittingly install the product when they install something else. A common way to become a victim of spyware is to download certain peer-to-peer file swapping products that are available today.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

**Startup items**

Any files placed in this folder will open when the computer starts. For example, a startup screen, a sound file to be played when the computer first starts, a reminder calendar, or application programs can be startup items. Normally, an alias of a file is placed in this folder rather than the file itself.

**System tray**

Introduced with Windows 95, the system tray is located in the Windows taskbar (usually at the bottom next to the clock) and contains miniature icons for easy access to system functions such as fax, printer, modem, volume, and more. Double click or right-click an icon to view and access the details and controls.

**TCP/IP**

Transmission Control Protocol/Internet Protocol - A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.

**Trojan**

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

The term comes from a story in Homer's Iliad, in which the Greeks give a giant wooden horse to their foes, the Trojans, ostensibly as a peace offering. But after the Trojans drag the horse inside their city walls, Greek soldiers sneak out of the horse's hollow belly and open the city gates, allowing their compatriots to pour in and capture Troy.

**Update**

A new version of a software or hardware product designed to replace an older version of the same product. In addition, the installation routines for updates often check to make sure that an older version is already installed on your computer; if not, you cannot install the update.

Bitdefender has it's own update module that allows you to manually check for updates, or let it automatically update the product.

**Virus**

A program or piece of code that is loaded onto your computer without your knowledge and runs against your will. Most viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can copy itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

**Virus signature**

The binary pattern of a virus, used by the antivirus program to detect and eliminate the virus.

**Worm**

A program that propagates itself over a network, reproducing itself as it goes. It cannot attach itself to other programs.